UNIVERSAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES



APLICACIÓN DE LA INFORMÁTICA FORENSE COMO BASE DE UNA PROPUESTA DE PROTOCOLO PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN EN LOS DELITOS INFORMÁTICOS EN GUATEMALA

GERARDO ESTUARDO DE LEÓN TARACENA

GUATEMALA, MARZO DE 2018

UNIVERSAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

APLICACIÓN DE LA INFORMÁTICA FORENSE COMO BASE DE UNA PROPUESTA DE PROTOCOLO PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN EN LOS DELITOS INFORMÁTICOS EN GUATEMALA

TESIS

Presentación a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

GERARDO ESTUARDO DE LEÓN TARACENA

Previo a conferirle el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, marzo de 2018

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	Lic.	Gustavo Bonilla
VOCAL I:	Lic.	Luis Rodolfo Polanco Gil
VOCAL II:	Licda.	Rosario Gil Pérez
VOCAL III:	Lic.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Jhonathan Josué Mayorga Urrutia
VOCAL V:	Br.	Freddy Noé Orellana Orellana
SECRETARIO:	Lic.	Fernando Antonio Chacón Urízar

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera fase:

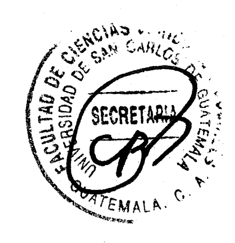
Presidente:	Licda.	Rosa María Ramírez Soto
Vocal:	Lic.	Luis Estrada Valenzuela
Secretario:	Lic.	Sergio Roberto Santizo Girón

Segunda Fase

Presidente:	Licda.	Aracely Amparo de la Cruz García
Vocal	Licda.	Diana Maribel Julián Leal
Secretaria:	Licda.	Dilia Estrada García.

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y contendido de la tesis". (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).





Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 21 de julio de 2017.

Atentamente pase al (a) Profesional, **OTTO ALBERTO POLANCO TOBAR** , para que proceda a asesorar el trabajo de tesis del (a) estudiante **GERARDO ESTUARDO DE LEÓN TARACENA**, con carné **201210984**, intitulado **APLICACIÓN DE LA INFORMÁTICA FORENSE COMO BASE DE UNA PROPUESTA DE PROTOCOLO PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN EN LOS DELITOS INFORMÁTICOS EN GUATEMALA.**

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA FAC. DE C.C. J.J. Y S.S. UNIDAD DE ASESORIA DE TESIS GUATEMALA, C. A.

LIC. ROBERTO FREDY ORELLANA MARTÍNEZ
Jefe(a) de la Unidad de Asesoría de Tesis

LIC. OTTO ALBERTO POLANCO TOBAR
ABOGADO Y NOTARIO

Fecha de recepción 25 / 08 / 2017 . f)

Asesor(a)
(Firma y Sello)



Lic. Otto Alberto Polanco Tobar
Abogado y Notario
39 av. 17-92 zona 6, Alamedas de Yumar
Mixco, Guatemala
Colegiada 9832

Guatemala, 10 de noviembre de 2017

Licenciado
Roberto Fredy Orellana Martínez
Jefe de la Unidad de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
15 NOV. 2017
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Distinguido licenciado:

Con fecha veintiuno de julio del año dos mil diecisiete mediante providencia correspondiente, fui designado asesor de tesis del bachiller Gerardo Estuardo de León Taracena. Cuyo título quedo así: intitulado **"APLICACIÓN DE LA INFORMÁTICA FORENSE COMO BASE DE UNA PROPUESTA DE PROTOCOLO PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN EN LOS DELITOS INFORMÁTICOS EN GUATEMALA".**

I. Declaro que no me une ningún parentesco dentro de los grados de ley, con el estudiante referido.

II. El ponente puso de manifiesto su capacidad de investigación en la elaboración del trabajo, aceptó diligentemente las sugerencias que durante el desarrollo del mismo le realice habiendo consultado interesante bibliografía con tópicos relacionados al tema, por ello el trabajo elaborado por el estudiante es meritorio, acucioso y demuestra interés en resolver el problema planteado.

III. El ponente hizo uso en forma amplia del método científico, abarcando las etapas del mismo y de esa manera comprueba fehacientemente la hipótesis planteada, utilizando el método deductivo y el método analítico, sintetizado adecuadamente lo analizado.

IV. La redacción utilizada reúne las condiciones exigidas en cuanto a claridad y precisión de tal manera que sea comprensible al lector.

V. En cuanto a la conclusión discursiva, es correcta y oportuna, plantea los conflictos encontrados en el desarrollo de la investigación, y se proponen soluciones viables para los mismos. Por lo que en virtud de lo anteriormente expuesto procedo a:

DICTAMINAR

Doy a conocer que el trabajo de tesis del bachiller, Gerardo Estuardo de León Taracena, cumple de manera eficaz con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura de Ciencias Jurídicas y Sociales y del Examen General Público, por lo que DICTAMINO FAVORABLEMENTE para que pueda continuar con el trámite respectivo, y para que pueda evaluarse posteriormente, por el tribunal examinador en el examen público de tesis, previo a optar al grado académico de licenciado en Ciencias Jurídicas y Sociales. Sin otro particular, me suscribo de usted.

Atentamente

LIC. OTTO ALBERTO POLANCO TOBAR
ABOGADO Y NOTARIO

Lic. Otto Alberto Polanco Tobar
Abogado y Notario
Colegiado 9832

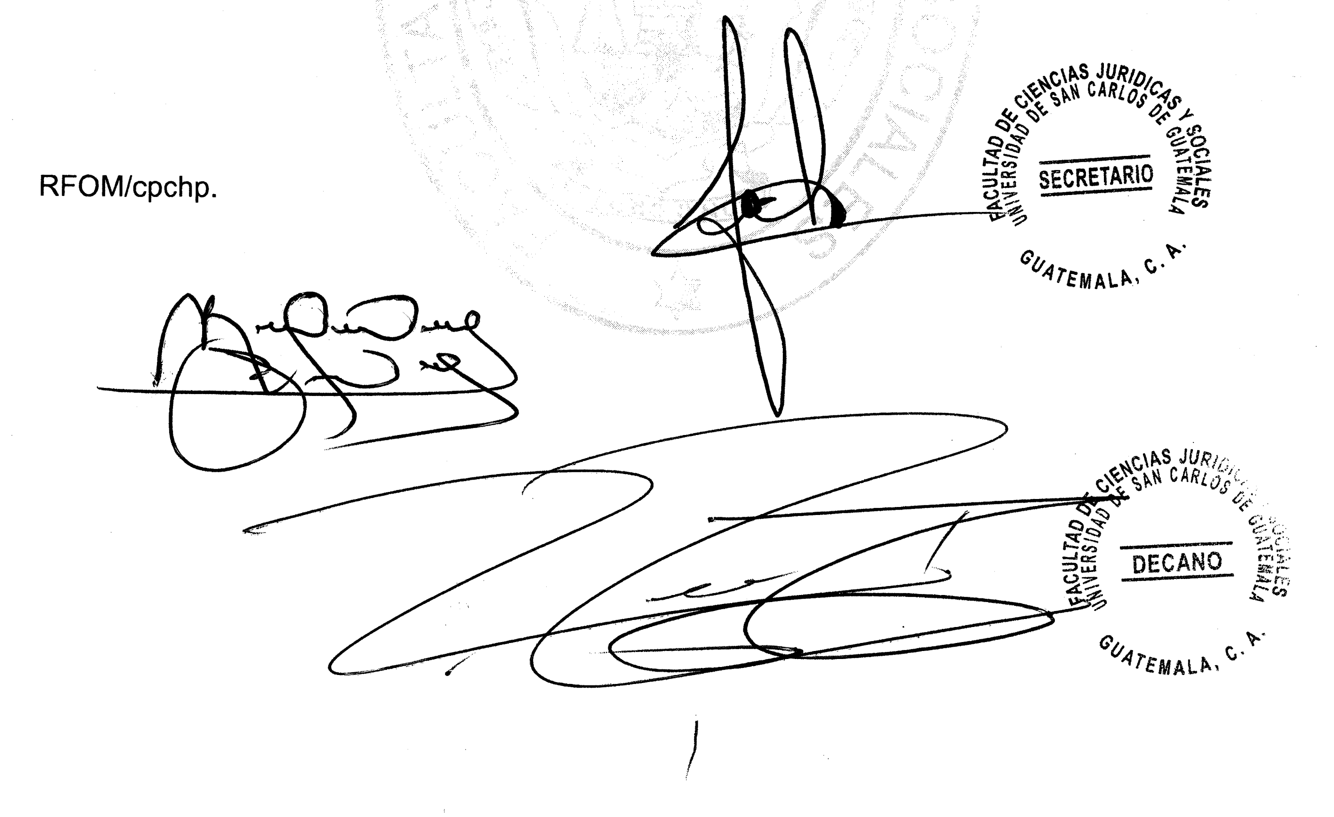




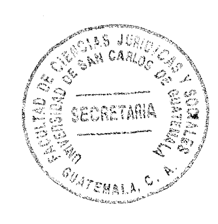
DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 14 de febrero de 2018.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante GERARDO ESTUARDO DE LEÓN TARACENA, titulado APLICACIÓN DE LA INFORMÁTICA FORENSE COMO BASE DE UNA PROPUESTA DE PROTOCOLO PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN EN LOS DELITOS INFORMÁTICOS EN GUATEMALA. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

RFOM/cpchp.







DEDICATORIA

A DIOS: Por permitirme llegar a este momento, y por estar a mi lado en todo momento; no importando lo difícil del camino, su presencia y amor impulsa cada paso.

A LA VIRGEN MARÍA: Por ser el modelo de madre y por interceder ante tu hijo Jesucristo en todo lo que en ti confiamos.

A MIS PADRES: Cesar Augusto de León Barrios y Suyapa María Taracena Pérez de de León, por ser el apoyo incondicional en todo momento y por el esfuerzo que siguen realizando día a día, no tengo palabras para agradecerles todo, este triunfo es de ustedes.

A MIS HERMANOS: Suyapa Renatta, Jorge Augusto, Andrea Paulina y Cesar Andrés, Gracias por ser mis compañeros de vida y por ser mi apoyo en momentos difíciles.

A MIS ABUELOS: Especialmente a Teresita del Niño Jesús Pérez Ordoñez (Q.E.P.D), estoy seguro que desde el cielo me acompañas en este logro, agradezco tu amor y la vida que compartimos.

A MIS TÍOS: Especialmente a Carolina Taracena, Sandra Taracena y Gerardo Taracena y Guadalupe de León, gracias por ser parte de mi formación, mi cariño, respeto y admiración.

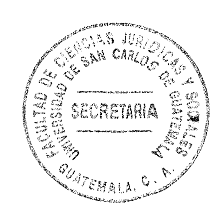
A MIS PRIMOS En especial a Mane Mérida, Jaqueline Mérida, Carol Mérida, Mario Mérida y Christian Álvarez, gracias por ser parte importante de mi vida, espero que sigamos compartiendo nuestros triunfos.

A MIS SOBRINOS: Javier Molina, Alejandro Molina, Alisson de la Cruz y Bastian de la Cruz, gracias por alegrar mi vida con su presencia.

A MI NOVIA: Vania Mariví Paiz Hernández, gracias por estar a mi lado siempre y por animarme día con día a ser una mejor persona. Te amo

A MIS AMIGOS: Por ser estos hermanos que la vida me puso en el camino, gracias por compartir sus sueños conmigo, especialmente a: Mónica Gonzalez, Anna Cermeño, Javier Díaz, Fredy Martínez, Rubén Méndez, Andrea González, Eduardo López, Eduardo Mazariegos, Carlos Velasquez, y Mishell Batres.

A : La Universidad de San Carlos de Guatemala, en especial a la Facultad de Ciencias Jurídicas y Sociales y a la jornada matutina, por recibirme en sus aulas y haberme formado como profesional.



PRESENTACIÓN

El objeto de estudio de la presente investigación y cuyos resultados se presentan, es la informática forense y su aplicación en la recolección de evidencia digital en las escena del crimen de los delitos informáticos. El sujeto de estudio de dicho trabajo son las personas encargadas de realizar la investigación criminal, con la cual se inicia la persecución penal, en este caso es el Ministerio Público. La investigación que se realizó es de carácter cualitativo y pertenece a la rama del derecho procesal penal la cual se desarrolló en el año 2017 circunscribiéndose conforme a la legislación vigente en el Estado de Guatemala.

El resultado de la presente tesis representa un aporte académico, ya que en el desarrollo de la presente, logre demostrar la importancia que tiene la correcta aplicación de la informática forense en la recolección de evidencia digital en la escena del crimen. En la actualidad, la informática ha permitido un avance en el desarrollo de nuevas formas de comunicación y desarrollo de las personas, pero ha traído nuevas formas de comisión de hechos ilícitos, por lo que el trabajo elaborado cobra vigencia. El correcto manejo de la escena del crimen y de las evidencias digitales es vital para la correcta investigación del hecho ilícito y por tanto del ejercicio de la acción pública penal que tiene el Ministerio Público



HIPÓTESIS

En el Estado de Guatemala, la entidad encargada de la investigación criminal es el Ministerio Público, sin embargo, cuando se da la recolección de la evidencia digital, por su volatilidad, se tiende a interrumpir de forma perjudicial a la investigación la cadena de custodia. Por tanto, es necesaria la implementación de un protocolo en el cual se evidencie una correcta metodología de recolección de evidencia digital conforme a los conocimientos técnicos de la informática forense.

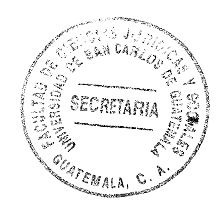
Para generar mi hipótesis, me basé en el objeto de estudio, el cual es la aplicación de la informática forense en la recolección de evidencia digital en la escena del crimen de los delitos informáticos, teniendo como sujeto de estudio los investigadores y fiscales del Ministerio Público. Las variables que se utilizaron en el presente trabajo de investigación son las independientes, la hipótesis es descriptiva y se desarrolló conforme al ordenamiento del Estado de Guatemala en el año 2017.



COMPROBACIÓN DE LA HIPÓTESIS

La hipótesis de la presente investigación fue comprobada contextualmente, ya que se demostró la necesidad de crear un protocolo en el cual se desarrolle un método de recolección de evidencia digital en la escena del crimen de los delitos informáticos, garantizando con ello la protección a la cadena de custodia de las evidencias. La hipótesis fue comprobada a través del método analítico, sintético y deductivo; se utilizaron las técnicas de investigación bibliográfica y documental.

El factor filosófico, utilizado en la argumentación de la hipótesis, se basa en el deber ser de la investigación criminal, puesto que en el caso de delitos informáticos, con la propuesta de regulación de un método para recolección de evidencias, se busca que los investigadores y quienes dirigen las diligencias en la escena del crimen tengan un sustento uniforme para el desarrollo de su trabajo en el lugar de los hechos. Por lo anterior descrito la hipótesis quedo validada con la presente investigación.



ÍNDICE

Pág.

CAPÍTULO I

CAPÍTULO II

Pág.

CAPÍTULO III

INTRODUCCIÓN

La informática forense, como una disciplina auxiliar de la administración de justicia, aplica conocimientos técnicos de la informática con el objeto de aplicarlos a la investigación criminal de hechos cometidos a través de un medio electrónico. Todo ello adquiere relevancia en el proceso de averiguación de la verdad que debe realizar el Ministerio Público, de acuerdo al sistema acusatorio, dentro del proceso penal. Elegí este tema por la relevancia que adquiere la informática en todos los aspectos de vida del hombre y el derecho no es la excepción.

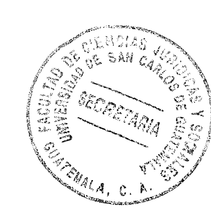
La hipótesis que se desarrolló gira en torno a la necesidad de implementar un protocolo en el cual se evidencie una correcta metodología de recolección de evidencia digital conforme a los conocimientos técnicos de la informática forense. Dicha hipótesis planteada fue contextualmente comprobada. Los métodos que se utilizaron en la presente investigación fueron el analítico, sintético y deductivo, mientras que la técnica que se utilizo en el presente trabajo fue bibliográfico.

Los objetivos que se alcanzaron en el desarrollo del presente trabajo fue la de determinar la metodología idónea para recolección de evidencias digitales en la escena del crimen; explicar a partir de los principios de la criminalística, la correcta protección de la cadena de custodia de las evidencias para presentarlas como medios de prueba y la exposición de los conceptos básicos de la informática forense como base de la metodología de recolección de evidencia digital. La investigación que se desarrolló pertenece tanto a la rama del derecho procesal penal, como a la disciplina de la

criminalística en la cual destacan términos como informática forense, evidencia digital y la cadena de custodia para la presentación de pruebas en el debate.

En el primer capítulo, se desarrolla el tema del derecho procesal penal, tanto como sus garantías constitucionales, los sujetos procesales que intervienen y el desarrollo del proceso penal; en el segundo capítulo, se establecen los delitos informáticos analizando los tipos penales actuales y los que se encuentran en discusión en el Congreso de la República de Guatemala; en el tercer capítulo, se analiza el tema de la criminalística partiendo de conceptos fundamentales, su evolución histórica, los principios que la conforman esta disciplina y el procesamiento de la escena del crimen; en el último capítulo, se determina la correcta aplicación de la informática forense en la recolección de evidencia digital en la escena del crimen de los delitos informáticos en el cual se analiza esta disciplina en función a la creación de metodologías que garanticen la protección de la cadena de custodia de la evidencia digital.

Esta investigación culminó con la comprobación de la hipótesis, en la cual se propone la creación de un protocolo de manejo de evidencia digita, por lo que el presente trabajo alcanzó su objetivo trazado.



CAPÍTULO I

1. Derecho procesal penal

Para que el Estado pueda castigar las conductas socialmente relevantes establecidas como delitos o faltas, es necesario establecer una serie de pasos ordenados por medio de los cuales el Estado aplicará el poder punitivo; a esto le llamamos proceso penal. El derecho procesal penal se encarga de desarrollar el proceso penal a través de principios, instituciones, normas jurídicas, doctrinas y jurisprudencia.

1.1. Definición

"El Derecho Procesal Penal es el conjunto de disposiciones legales sistemáticamente estructuradas que establecen coactivamente la organización, formas y medidas de actuación del poder jurisdiccional del Estado para la aplicación o realización del Derecho Penal Sustantivo, fijando procedimientos que regulen, garantizando los derechos individuales, la investigación judicial y los debates entre las partes, con miras a la declaración de certeza en torno a la comisión de hechos delictivos generadores de pretensión punitiva y eventualmente resarcitoria, y las posteriores ejecuciones "[1].

El objeto de estas disposiciones legales es regular el proceso y las relaciones jurídicas que crean a partir de la realización penal y sus consecuencias jurídicas, siendo sus destinatarios el juez y sus auxiliares, el Ministerio Público, las partes privadas y aquellos

[1] Vazquez Rossi, Jorge Eduardo. **El derecho procesal penal (La realización penal) Tomo I**, Pág. 39.

llamados a colaborar en la administración de justicia como los testigos, peritos, etcétera. Es decir, si el derecho penal se encarga de regular el nacimiento de la pretensión penal estatal, el derecho procesal penal se ocupa de cómo el Estado aplicará la pretensión penal.

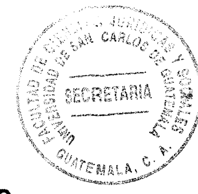
1. 2. Garantías procesales constitucionales

La Constitución Política de la República de Guatemala para la protección de la persona sometida a un proceso penal, configura una serie de garantías por medio de las cuales se limita el poder Estatal frente al imputado. Estas garantías pretenden evitar la violación de derechos fundamentales ya que "Las garantías constitucionales son los medios técnico-jurídico, orientados a proteger las disposiciones constitucionales orientados a proteger las disposiciones constitucionales cuando estas son infringidas, reintegrando el orden jurídico violado."[2]

Dichas garantías son:

Debido proceso o juicio previo: "Constituye un límite a la actividad estatal, se refiere al conjunto de requisitos que deben observarse en las instancias procesales a efectos de que las personas estén en condiciones de defender adecuadamente sus derechos ante cualquier acto del Estado que pueda afectarlos"[3]. Esta garantía se encuentra regulada en la Constitución Política de la República de Guatemala en el Artículo 12 establece:

[2] García Laguadia, Jorge Mario. **La defensa de la constitución**. Pág. 24.
[3] García Ramírez, Sergio. **El debido proceso** Pág. 22.



"...Nadie podrá ser condenado, ni privado de sus derechos, sin haber sido citado, oído y vendido en el proceso legal ante juez o tribunal competente y preestablecido..."

Presunción de Inocencia: Esta garantía se configura como "un principio fundamental del Derecho Procesal Penal que informa la actividad jurisdiccional como regla probatoria y como elemento fundamental del derecho a un juicio justo."[4] Por esta garantía se reconoce que el imputado goza de la misma situación jurídica que un inocente, por tanto no debe. La Constitución Política de la República de Guatemala en el Artículo 14 indica: "Toda persona es inocente, mientras no se le haya declarado responsable judicialmente, en sentencia debidamente ejecutoriada..."

Derecho de defensa: Consiste en la necesidad jurídica y material que tiene toda persona que se encuentra sometida a un proceso jurisdiccional de salvaguardar sus intereses, en condiciones de igualdad. "La defensa adecuada entraña una prohibición para el Estado, consistente en no entorpecer el ejercicio del derecho de defensa del gobernado y un deber de actuar." [5] La defensa de una persona generalmente recae en un profesional del derecho, específicamente un abogado. En relación directa al derecho de defensa la Constitución Política de la República de Guatemala en el Artículo 12 indica: "La defensa de la persona y sus derechos son inviolables..."

Derecho e igualdad de las partes: "La igualdad requiere, para su existencia en el proceso penal, de un sistema garantista y bajo el cobijo del principio de contradicción,

[4] Aguilar García, Ana Dulce. **Presunción de inocencia.** Pág. 15.
[5] Cruz Barney, Oscar. **Defensa a la defensa y abogacía en México.** Pág. 12.

con ello, se busca que los sujetos en proceso penal cuenten con los medios necesarios para presentar sus respectivas posiciones, pretensiones, y puedan generar con ello, las condiciones de debate, para que puedan ser oídos y vencidos en juicio."[6] Es entendido que el Ministerio Público, el imputado y su defensa, la víctima y el agraviado cuentan con las mismas prerrogativas y oportunidades dentro del proceso penal. En la Constitución Política de la República de Guatemala, la igualdad se encuentra regulada en el Artículo 4.

1.3. Sistemas procesales

Para la Real Academia de la Lengua española la palabra sistema significa: "Conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí."[7] En el caso de los sistemas procesales, este conjunto de reglas y principios giran en torno a la persecución penal por la posible comisión de hechos considerados como delitos o faltas. Los sistemas procesales son "el conjunto de disposiciones y de maneras operativas, empleadas dentro de una sociedad para resolver (averiguar y decidir) un conflicto de índole penal."[8] El conflicto de índole penal se centra en la investigación de la responsabilidad de un sujeto

Cada sistema procesal cuentan con una serie de rasgos determinantes, los cuales son característicos de modos históricos de enjuiciamiento. En cada sistema se desarrollan

[6] Santacruz Luma, Rafael. **El principio de igualdad entre las partes en el proceso penal en México.** Pág. 138.
[7] http://www.dle.rae.es/?id=Y2AFX5s (consultado 15 de septiembre de 2017).
[8] Vázquez Rossi. **Op. Cit**. Pág. 187.

actividades procesales, en los cuales el juez y las partes encuentran limitada su actuación dentro del proceso penal. Los sistemas procesales que de forma antagónica han existido son el sistema inquisitivo y el sistema acusatorio, los cuales son un reflejo de una realidad social y cultural de determinado tiempo y determinado lugar.

1.3.1. Sistema inquisitivo

El contexto político y cultural en el cual surge el sistema inquisitivo, es un régimen autoritario, muchas veces existiendo la unión entre el Estado y la Iglesia en el cual el delito se entiende como "Consustancial a la de desacato o incumplimiento de la autoridad y sus mandatos; y la persecución de una forma de ser, de una personalidad (el cristiano para los romanos; el hereje, el réprobo, el cismático, los judíos, los falsos conversos luego)."[9] Es decir, la persecución penal gira en torno a la forma de ser del delincuente y no al hecho o conducta prohibida.

La averiguación se extiende a la averiguación de la verdad real y el proceso averiguativo es secreto y desconfía de toda explicación o excusa defensiva. El uso sistemático de la intimidación y la provocación de dolor son características del proceso investigativo, puesto que se sostiene que la sospecha tiene como consecuencia el castigo y el sufrimiento es como una forma expiativa. "En el fondo del proceso inquisitivo anida una idea maniquea: el bien, los valores, pertenecen al Estado; el mal está en los individuos que han infringido, de cualquier modo, los mandatos

[9] Ibíd. Pág. 203.




soberanos.”[10]

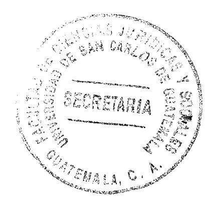
La iniciación de la acción penal es de oficio, en las cuales los órganos oficiales permanentes y especializados en la persecución, investigación y juzgamiento tienen una vinculación directa. Existe confusión entre la acción y jurisdicción, puesto que la persecución penal publica “es ejercida por el inquisidor que es, a la vez, meritador de sus propios actos, parte actora y juez.”[11] La denuncia tiene la función de hacer llegar datos a la autoridad, quien debe iniciar la investigación, la cual parte de una declaración de una persona identificable o de forma anónima.

Las características del sistema inquisitivo son: Existe confusión entre acción y jurisdicción, ya que no hay partes procesales y el derecho de defensa está limitado , la iniciación se da de oficio por el propio tribunal ante noticia de delito; El desarrollo del proceso es discontinuo, puesto que los actos se documentan por escrito y la investigación es secreta; existe una regulación estricta sobre la prueba a través de la prueba legal o tasada; el imputado es el objeto de la investigación, y limita la posibilidad de actuación y finalmente los jueces son protagonistas del proceso ya que son los que manejan la investigación.

El sistema inquisitivo tiene su origen en la necesidad que han tenido a lo largo de la historia los Estados, para alcanzar un mayor fortalecimiento, a través de la persecución de todo aquello que pueda constituir un peligro para la sociedad.

---

[10] **Ibíd.** Pág. 204.
[11] **Ibíd.** Pág. 206.



1.3.2. Sistema acusatorio

El contexto político y cultural en el cual aparece este sistema es durante un régimen democrático, en el cual se da la participación ciudadana, intervención y control popular sobre los actos Estatales. El derecho penal se centraliza en la conducta y ya no en la de la forma de ser del delincuente. La atribución y la responsabilidad se limitan a lo que las partes puedan postular, acreditar o alegar en una situación de igualdad

El delito se configura como un daño o infracción a las leyes comunitarias, es un hecho público que atenta contra las bases de la convivencia, interesa y concierne a todos; el juez representa la pretensión popular. El proceso se inicia y desarrolla a través de la acción; y la acusación se describe como "la acción con un contenido de pretensión punitiva, dirigida de manera concreta hacia el accionado o acusado, estableciendo entre estos una relación procesal entre ambos"[12]. La acusación puede ser pública o privada; La acusación es pública cuando se promueve por cualquier persona y se da en casos de delitos públicos; y es privado cuando se promueve únicamente por el afectado del delito.

"El sistema acusatorio se define y caracteriza por la firme diferenciación de los poderes de acción y jurisdicción, conformando una especial relación procesal de horizontalidad contradictoria entre actor y accionado y de verticalidad con el órgano jurisdiccional." Esto permite al acusado el legítimo ejercicio de defensa frente a la pretensión punitiva

[12] **Ibíd.** Pág. 191.

de la parte acusadora. La jurisdicción se presenta como una manifestación de la democracia, ya que representa la pretensión del pueblo."[13]

Las características del sistema acusatorio son: en relación a la organización institucional. Existe ausencia de aparatos oficiales judiciales de persecución penal; Existe contradictorio, puesto que hay partes antagónicas en el proceso los cuales están en igualdad de condiciones de aportar pruebas y oponerse a la pretensión de la otra; la iniciación del proceso es a través de un acto formal de acusación; el proceso se da por medio de audiencias orales en la cual las partes discuten frente al órgano jurisdiccional; Existe libertad probatoria de las partes; el imputado se considera como un sujeto de derechos y la actitud del juez es pasiva, puesto que solo se encarga de intermediar entre las partes del contradictorio y se encarga de controlar la investigación.

1.4. Sujetos procesales

Los sujetos procesales son aquellas personas individuales o jurídicas, capaces legalmente para formar parte de un proceso contradictorio en la cual se lleva a cabo una relación jurídica procesal que gira en torno a un hecho delictivo y que tiene por objeto la averiguación de la verdad.

Los sujetos que intervienen en el proceso penal son diversos, pero cada uno desarrolla una actividad importante dentro del desarrollo de la misma. El Ministerio Público y los órganos auxiliares de investigación, El imputado y su defensa, el tercero civilmente

[13] **Ibíd**. Pág. 193.

demandado, la victima como querellante adhesivo y el querellante exclusivo son ejemplos de estos sujetos procesales.

"En el proceso penal necesariamente han de existir dos sujetos que mantienen posiciones contrapuestas, sin cuya concurrencia no se puede entrar en el juicio, de modo que cuando no haya contradicción (porque el órgano público inste la absolución del inocente o pida el sobreseimiento), finaliza el proceso o no se llegará abrir." [14] Estos sujetos son llamados en la doctrina como partes; ya que hay diversidad de sujetos dentro de un proceso pero únicamente deben de existir dos partes en un proceso contencioso, como lo es el proceso penal.

La parte actora o acusadora es la que solicita al órgano jurisdiccional la aplicación de una condena por un hecho calificado como delito o falta; la parte pasiva o acusada es la que se defiende. Los sujetos acusadores en el proceso penal son: Ministerio Público, querellante adhesivo y el querellante exclusivo; Los sujetos acusados son el Imputado y el tercero civilmente demandado acompañados estos por su defensa técnica.

1.4.1 Ministerio Público y los órganos auxiliares

Es una institución auxiliar de la administración pública y de los tribunales, la cual tiene a su cargo el ejercicio de la acción penal pública así como la de velar por el estricto cumplimiento de las leyes del país, ejerce sus funciones de forma autónoma en relación a su organización y su funcionamiento. "Esta autonomía es delegada como un

[14] Poroj Subuyuj, Oscar Alfredo. **El proceso penal guatemalteco. Tomo I.** Pág. 112.

contrapeso para que en realidad la institución pueda llevar a cabo con independencia y rigor técnico la investigación de todos aquellos delitos de acción pública, de oficio o a instancia particular, que tenga conocimiento consagrado así en un proceso penal contradictorio, sustentado en la estricta sedación de funciones: la de investigar, que corresponde al Ministerio Público y la de juzgar atribuida con exclusividad al Órgano jurisdiccional."[15]

La Ley Orgánica del Ministerio Público, Decreto 40-94 del Congreso de la República de Guatemala, indica que las funciones de dicha institución son: Investigar los delitos de Acción pública y promover la persecución penal ante los tribunales; Dirigir a la policía y demás cuerpos de seguridad del Estado en la investigación de hechos delictivos y preservar el Estado de derecho y el respeto a los derecho humanos, efectuando las diligencias necesarias ante los tribunales de justicia. Estas funciones se orientan según los principios de Unidad, jerarquía y objetividad establecidos en el ordenamiento jurídico vigente en el Estado de Guatemala.

Los auxiliares del Ministerio Público en la investigación son:

a) La Policía Nacional Civil: La Ley de la Policía Nacional Civil, Decreto 11-97 del Congreso de La República de Guatemala, establece en el Artículo dos que: "Es una institución profesional armada, ajena a toda actividad política. Su Organización es de naturaleza jerárquica y su funcionamiento se rige por la más estricta disciplina..." Está a cargo del Presidente de la República, a través del Ministerio de Gobernación y su

---

[15] Rodriguez Barillas, Alejandro. **Manual de derecho procesal penal II.** Pág. 5.

funcionamiento a cargo del Director General, y supeditado a la inmediación y exclusiva autoridad del Ministerio de Gobernación."[16]

Sus funciones dentro del proceso penal es: investigar los hechos punibles perseguidos de oficio, impedir que estos sean llevados a consecuencia ulteriores, individualizar a los sindicados y reunir los elementos de investigación útiles para dar base a la acusación o determinar el sobreseimiento . Todas estas funciones pueden ser iniciadas por iniciativa propia o por orden del Ministerio Público.

b) Victima y querellante adhesivo: La declaración de los principios fundamentales de justicia para las Víctimas de delitos y de abuso de poder, de la Organización de Naciones Unidas, define a las víctimas de delito de la siguiente forma: Se entenderá por víctimas las personas que individual o colectivamente, hayan sufrido daños, incluido lesiones físicas o mentales, sufrimiento emocional, pérdida financiera o menoscabo sustancias de sus derechos fundamentales, como consecuencia de acciones u omisiones que violen la legislación penal vigente en los Estados Miembros, incluida la que proscribe el abuso de poder.

La participación de la víctima dentro del proceso penal debe formalizarse a través de su constitución como querellante adhesivo, con el objeto de hacer valer sus derechos dentro el juicio penal; No obstante el Código Procesal Penal no utiliza el concepto de víctima, sino el de agraviado; el cual es más amplio, ya que sirve para identificar quienes tienen legitimidad para intervenir en el proceso penal. En los delitos de acción

---

[16] **Ibíd.** Pág. 25.

pública, el agraviado o su representante pueden provocar la persecución penal o adherirse a la ya iniciada por el Ministerio Público.

c) El querellante exclusivo: es la persona individual o jurídica la cual tiene a su cargo la persecución penal de los delitos de acción privada.

1.4.2. El imputado y su defensor

El Artículo 70 del Código Procesal Penal, Decreto 51-92 del Congreso de la República de Guatemala, establece: "Se denominará sindicado, imputado, procesado o acusado a toda persona a quien se le señale de haber cometido un hecho delictuoso, y condecorado a aquél sobre quien haya recaído una sentencia condenatoria firme." El imputado es cualquier persona contra quien se dirige la pretensión punitiva por la participación en un hecho considerado como delito o falta.

"El imputado es uno de los sujetos procesales fundamentales. Tiene dentro del procedimiento una posición pasiva en relación al objeto procesal y en relación a los llamados sujetos activos (fiscal y querellante)."[17] El imputado se encuentra en una situación pasiva dentro del proceso penal, no obstante puede actuar dentro del proceso, por su derecho de defensa. Existen limitaciones físicas y técnicas del imputado dentro del proceso penal. Las limitaciones físicas o materiales son el resultado de las medidas de coerción o de la imposibilidad material de participar con un control activo en las diligencias que el Ministerio Público realice en su contra. Las limitaciones técnicas son

[17] **Ibíd.** Pág. 66.

aquellas que padece el imputado por su posible ignorancia sobre aspectos técnicos – jurídicos sobre el desarrollo del proceso penal.

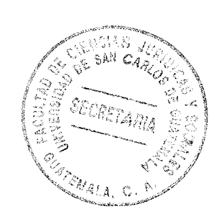
El derecho de defensa constituye una garantía fundamental, ya que el imputado goza del status de inocencia, que le permite oponerse a la pretensión en su contra, ya que puede refutar la acusación o los actos en los cuales se basa esta, indicar las deficiencias formales dentro del procedimiento. De forma sintética, el derecho de defensa se define como aquel derecho básico del imputado de no estar sometido a actividad oficial abusiva, ya que la persecución penal debe estar regida por la legalidad y todos sus operadores deben someterse a su puntual cumplimiento. La defensa puede ser material o técnica. La segunda es derivación de la primera.

"La defensa material es aquella realizada del modo personal e insustituible por el propio imputado y se manifiesta principalmente en todos aquellos actos que realiza por sí, tales como sus declaraciones, tanto en la etapa investigativa como durante el juicio; en la reconstrucción de los hecho, reconocimiento de personas y/o elementos probatorios, y careos con otros imputados y/o testigos."[18]

La defensa material recae sobre el mismo imputado, pero esta se encuentra limitada, ya que existen distintos actos procesales en los cuales es necesario conocimientos técnicos-jurídicos los cuales si el imputado no es profesional del derecho, es imposible que realice su defensa. Por lo anterior descrito surge la defensa técnica, ejercida por el defensor.

---

[18] Vazquez Rossi, Jorge Eduardo, **El derecho procesal penal (La realización penal) Tomo II**, Pág. 86.



El defensor técnico es el profesional del derecho, abogado, que tiene a tiene a su cargo la defensa técnica-jurídica del imputado. El imputado debe de proveerse, o el Estado debe designarle, de un defensor con el objeto de ser asistido y representando en todas las actuaciones dentro del proceso y actuando en función de sus intereses. "La designación de defensor es un acto de defensa material que corresponde de manera exclusiva al imputado, quien tiene esta facultad a lo largo de todas las instancias del proceso."[19] La defensa técnica puede estar a cargo de un defensor particular o de confianza, defensor de oficio y el defensor del Instituto de la Defensa Pública Penal.

1.5. El órgano jurisdiccional

La jurisdicción es la "facultad conferida a determinados órganos para la interpretación y aplicación del Derecho en los supuestos en que se produce una insatisfacción, conflicto o desobediencia en relación a las normas objetivas."[20] La función jurisdiccional es la actividad de mantenimiento del orden jurídico cuando el mismo ha sido desobedecido, cuestionado o invocado concretamente en defensa de un derecho o interés tutelado e insatisfecho; esta función jurisdiccional es la que el Estado le delega a los órganos jurisdiccionales.

Órgano Jurisdiccional es "la corporación formada por funcionarios de diferente jerarquía y actuantes dentro de sus respectivas materias y regiones para dirigir proceso y

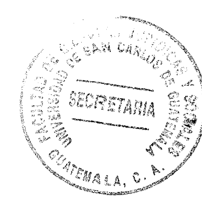
[19] **Ibíd.** Pág. 87.
[20] **Ibíd**. Pág. 107.

pronunciarse conforme a lo establecido en las normas generales del Derecho Sustantivo."[21] Según la Doctrina Romana, la jurisdicción cuenta con distintos poderes los cuales son necesarios para el desarrollo de su función; estos poderes son: *notio, vocatio, coertio, iudicium y executio.*

El poder de conocer (*notio*) en el cual el órgano jurisdiccional tiene la facultad de conocer de los conflictos sometidos a el; El poder de convocar (*vocatio*) el cual el órgano jurisdiccional cita a las partes a juicio; El poder de coerción (*coertio*) el cual consiste en la facultad que tiene el órgano jurisdiccional de decretar las medidas coercitivas cuya finalidad es remover aquellos obstáculos que se oponen al cumplimiento de la jurisdicción; El poder de decisión (*iudicium*) el cual es la facultad para decidir, y que esta decisión tenga carácter de cosa juzgada. Y el poder de ejecución (*executio*) el cual consiste en la facultad que tiene el órgano jurisdiccional para hacer cumplir sus resoluciones. Estos poderes los posee todo órgano juridiccional, para ejercer su función de administrar justicia.

La Jurisdicción se encuentra limitada por la competencia, ya que esta distribuye la actividad jurisdiccional por razón de materia, cuantía y territorio. En materia penal, los órganos jurisdiccionales que tienen competencia son: Los jueces de paz; los jueces de primera instancia; Los jueces unipersonales de sentencia; Los tribunales de sentencia; Los jueces de primera instancia por procesos de mayor riesgo; Tribunales de sentencia por procesos de mayor riesgo, Las salas de la corte de apelaciones, La Corte Suprema de Justicia y los jueces de ejecución.

[21] **Ibíd.** Pág. 116.



1.6. El proceso penal

"El proceso es el fenómeno jurídico mediante el cual sujetos habilitados para ello, determinan la aplicación del Derecho sustantivo en situaciones concretas en las cuales tal normatividad se ha postulado controvertida o inobservada recurriendo a procedimientos de acreditación y alegación con miras a la decisión que, de modo vinculante dictará el órgano jurisdiccional. Se trata de un sistema legalmente establecido que a través de los órganos judiciales y con intervención de sujetos habilitados u obligados, estructura una secuencia de actos que se desarrollan ordenadamente hacia la obtención del pronunciamiento jurisdiccional que determina coactivamente la aplicación al caso de la normatividad sustantiva pertinente."[22]

El proceso penal se define como "el conjunto de actos que órganos y sujetos determinados llevan a cabo a partir de la noticia de un suceso de apariencia delictiva que provoca la acción como promoción y desarrollo para arribar a una decisión final y vinculante que resuelve sobre la procedencia de una pretensión punitiva, que solo puede válidamente imponerse como consecuencia del juicio previo o debido proceso."[23]

El proceso se convierte en un método necesario para la aplicación de una pena, ya que está reconocido de forma constitucional y ordinaria por las garantías del debido proceso, del derecho de defensa, la garantía procesal las cuales están inspiradas en el principio de legalidad. El debate jurídico con miras a la correcta aplicación del Derecho

[22] Ibíd. Pág. 15
[23] Ibíd. Pág. 20



vigente es la sustancia del proceso penal.

El Artículo 5 del Código Procesal Penal, Decreto 51-92 del Congreso de la República de Guatemala, establece: "El proceso penal tiene por objeto la averiguación de un hecho señalado como delito o falta y de las circunstancias en que pudo ser cometido; el establecimiento de la posible participación del sindicado; el pronunciamiento de la sentencia respectiva, y la ejecución de la misma. La víctima o el agraviado y el imputado como sujetos procesales, tiene derecho a la tutela judicial efectiva. El procedimiento por aplicación del principio del debido proceso, debe responder a las legitimas pretensiones de ambos."

1.6.1. Etapa preparatoria

La primera etapa o fase del proceso penal en Guatemala es el procedimiento preparatorio. El procedimiento preparatorio tiene como objeto principal realizar la investigación preliminar de un delito, para reunir datos y elementos de prueba que permitan plantear una pretensión fundada. Esta etapa persigue practicar las diligencias pertinentes y útiles para determinar la existencia del hecho, partícipes, circunstancias para valorar la responsabilidad o que influyan en su punibilidad.

El objeto de la etapa preparatoria es reunir los medios de investigación en las cuales se determine la responsabilidad de un sujeto (imputado) en el hecho delictivo. Inicia con los actos introductorios o *notitia criminis* son las diferentes formas de comunicar ante el Ministerio Público, la Policía Nacional Civil o el juez, un hecho o un

acontecimiento que posiblemente constituya un delito. Los actos introductorios dentro del ordenamiento jurídico son: denuncia, querella, prevención policial y el conocimiento de Oficio.

Luego de la presentación de los actos introductorios, el Ministerio Público debe investigar y recabar los elementos de convicción, con base en el principio de objetividad. Si el Ministerio Público recaba la suficiente cantidad de medios de convicción para determinar la posible responsabilidad de un sujeto en un hecho delictivo y lo ha podido individualizar, a través del control jurisdiccional, solicita al juez la orden de detención o citación para que se lleve a cabo la audiencia de primera declaración.

La Audiencia de primera declaración tiene por objeto determinar si es necesario ligar a proceso penal al sindicado, en caso de ligar a proceso se discute sobre la aplicación de medidas de coerción y sobre el plazo para que el Ministerio Público investigue. La etapa preparatoria termina con la presentación del acto conclusivo, en el cual el Ministerio Publico puede presentar la acusación formal y petición de apertura a juicio, sobreseimiento, clausura provisional o la aplicación de medidas desjudicializadoras.

1.6.2. Etapa intermedia

Posterior a la etapa preparatoria, o investigación se encuentra la etapa intermedia, el cual tiene por objeto evaluar si existe la fundamentación para someter al imputado a juicio oral y público. Funciona como una fase de transición entre el procedimiento

preparatorio y la fase de debate. Está conformada por un conjunto de actos procesales que tienen como fin la corrección de los requerimientos o actos conclusivos de la investigación. "El procedimiento intermedio se funda en la idea de que los juicios de en ser preparados convenientemente y se debe llegar a ellos luego de una actividad responsable."[24]

Esta etapa se lleva a cabo a través de una audiencia, en la cual cobra importancia el principio contradictorio, en la cual se permite a la defensa técnica el asumir en igualdad de condiciones, las posiciones y argumentos. En esta audiencia se puede objetar la decisión del Ministerio Público, ya sea en contra de la acusación por parte de la defensa, en contra de la Clausura Provisional o Sobreseimiento en caso de la Victima constituida como querellante adhesivo.

1.6.3. Etapa de juicio o debate

"Si Luego del procedimiento intermedio se ha decidido aceptar la acusación se dará paso a la etapa o fase de juicio. Etapa que es la más importante de todo el procedimiento, pues es la que tiene como objetivo resolver en definitiva el conflicto que ha sido presentado al Estado para que busque una solución" [25] Esta tercera etapa es la ponencia del proceso en forma contradictoria, oral y pública, en la cual las partes entran en contacto directo. El contenido del proceso se manifiesta con toda su amplitud, se presentan y diligencian las pruebas.

[24] Rodríguez Barillas, Alejandro. **Op. Cit**. Pág. 81.
[25] **Ibíd**. Pág. 84.

Los medios de prueba son aquellos elementos que permiten el ingreso de toda información disponible, la cual será utilizada en el tribunal para dictar la sentencia en la cual el tribunal de sentencia o el juez unipersonal de sentencia determinara si existe o no participación del acusado en el hecho delictivo. El Órgano Jurisdiccional al dictar sentencia valorara la prueba según el criterio de la sana crítica razonada.

La importancia y fundamento del juicio oral recae en el mandato constitucional que ostenta nuestro ordenamiento penal, el cual indica el principio del debido proceso, en el que para ser condenado antes debe ser citado, oído y vencido en juicio. Los principios básicos del debate son: oralidad, inmediación, concentración, continuidad, publicidad, contradicción y el principio de congruencia.

CAPÍTULO II

2. Delitos informáticos

Los delitos informáticos son llamados delitos cibernéticos o delitos electrónicos y distintos autores los han definido así:

"Cualquier acto ilegal en relación con el cual, el conocimiento de la tecnología informática sea esencial para su comisión, investigación y persecución, es decir se utilice la tecnología informática para cometer el delito, que se utilice la tecnología informática para cometer el delito, que se utilice la tecnología informática para investigar el delito y que se utilice la tecnología informática para perseguir a los supuestos autores, cómplices o participes del hecho punible."[26]

"Acción u omisión, típica, antijurídica y culpable, que se realiza por medio de un sistema que haga uso de las tecnologías de la información o un componente de éste, o que lesione la integridad, disponibilidad o confidencialidad de la información."[27] "Es toda acción dolosa que cause un perjuicio a personas naturales o jurídica que puede producir o no un beneficio material para su autor, pudiendo o no perjudicar de forma directa o inmediata a la víctima, caracterizándose dicha acción por ser realizada mediante dispositivos habitualmente utilizados en actividades informáticas."[28]

---

[26] Eyner Isaza, Henry. **Medios electrónicos e Informáticos y su implementación al sistema penal acusatorio.** Pág. 40.
[27] Alvarado, Rolando; Morales, Ronald. **Cibercrimen.** Pág. 16.
[28] Solano, Orlando. **Manual de informática jurídica.** Pág. 277.

Definiremos los delitos informáticos como las acciones u omisiones en las cuales el sujeto activo utiliza un medio electrónico y/o digital para realizarlo, y afecta directamente la información en perjuicio de una persona en su derecho a la intimidad o su patrimonio.

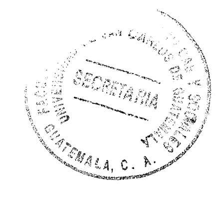
2.1. Características de los delitos informáticos

"Los delitos informáticos requieren indefectiblemente de los medios informáticos para su existencia. Podemos decir que los delitos informáticos poseen peculiaridades que los hacen de alguna manera sui generis, por un lado en cuanto a su forma de ejecución y, por otro, respecto de su detención o descubrimiento."[29] El delito informático se diferencia de los demás, por dos circunstancias: La primera, son las maniobras fraudulentas que se realizan por un medio electrónico y la segunda, el resultado del delito implica la obtención de información o datos en perjuicio de una persona. Las características comunes a los delitos informáticos son:

a) La rapidez en tiempo y la posición cercana al perjudicado; ya que estos pueden ser usados por una persona de forma rápida, ya que solo necesitará de una acción, como un clic, para ejecutar el hecho delictivo.

b) Facilidad para encubrir el delito; la rapidez con la que sucede el hecho delictivo y la distancia que existe entre el afectado y el sujeto activo del delito, permite facilitar las condiciones óptimas para encubrir el delito, ya que los sistemas de cómputo son fácilmente penetrables.

[29] Eyner Isaza, Henry. **Óp. Cit**. Pág. 45.



2.2. Bien jurídico tutelado en los delitos informáticos

El bien jurídico tutelado es el interés jurídicamente protegido; son intereses vitales, intereses del individuo o de la comunidad, estos intereses no son creación del ordenamiento sino de la vida, pero la protección jurídica eleva el interés vital a bien jurídico. "El bien jurídico protegido es el fundamento de la norma. La prohibición de una conducta y la imposición de una sanción, solo se justifica en cuanto sirvan para proteger un bien jurídico."[30] En los delitos informáticos es necesario proteger de forma particular:

a) La integridad, la disponibilidad y la confidencialidad; ya que los sistemas que utilizan tecnología de la información y sus componentes deben garantizar la certeza jurídica en las transacciones propias del comercio electrónico.

b) El software, para contrarrestar los ataques cibernéticos que tiendan a dañar el patrimonio de una persona.

Los bienes jurídicos tutelados que se pretender proteger con la determinación de los delitos informáticos son: la información y el patrimonio por su propia naturaleza, y la vida, la integridad sexual, el pudor, el honor y la seguridad nacional en relación a la forma en que pueden realizarse los delitos utilizando medios electrónicos. El bien jurídico de la información tiene relevancia puesto que se protege la información en cuanto a sus atributos de integridad, disponibilidad y confidencialidad.

---

[30] González Cauhapé-Cazaux, Eduardo. **Apuntes de derecho penal guatemalteco.** Pág. 41.

El patrimonio se protege toda vez que se sancionan todos aquellos actos de transferencia patrimonial no ha sido consentido por el propietario, así como lo relativo al daño informático.

2.3. Clasificación de los delitos informáticos

Por la forma en que se utiliza la computadora para cometer el ilícito, los delitos informáticos se dividen en:

a) Como instrumento o medio: "En esta categoría se encuentran las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito."[31] Este delito puede afectar: el patrimonio, la privacidad, la seguridad, la vida, la integridad personal, el honor y la seguridad.

b) Como fin u objeto: "En esta categoría encuadramos a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física."[32] Este delito puede afectar directamente el hardware y el software.

Según el bien jurídico que se pretende tutelar, la doctrina los clasifica en

a) Delitos contra la integridad: En esta categoría podemos encuadrar daño informático, falsificación informática y fraude informático.

---

[31] Alvarado, Rolando; Morales Ronald. **Op. Cit**. Pág. 16.
[32] Ibíd. Pag.16.

b) Delitos contra la disponibilidad: En esta categoría esta el delito de violación a la disponibilidad.

c) Delitos contra la confidencialidad: espionaje informático, acceso ilícito, reproducción de dispositivos de acceso, interceptación ilícita.

d) Delitos contra la persona: regulados en el Código Penal de Guatemala, Decreto 17-73 del Congreso de la República de Guatemala así como los delitos relacionados a la violencia sexual, explotación y trata de personas; así como el de difusión y alteración de imágenes personales y el del uso de identidad ajena.

f) Delitos contra la seguridad nacional: delitos contra la nación, actos de terrorismo informático.

2.4. Tipos penales

Un tipo penal es "la descripción de una conducta prohibida por una norma."[33] El tipo penal debe contener elementos objetivos y subjetivos. Los elementos del tipo objetivo son: el sujeto activo, el sujeto pasivo, la acción y el bien jurídico; Los elementos del tipo subjetivo son: que constituye el dolo o culpa con que se realiza la acción.

En el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala se regulan los siguientes conductas delictivas con relación a los medios informáticos.

[33] González Cauhapé-Cazaux, Eduardo. **Op. Cit.** Pág. 39.

a) Destrucción de registros informáticos: este delito consiste en destruir, borrar o de cualquier forma alterar o dañar registros informáticos y lo relaciona con una pena de prisión de de seis meses a dos años y multa de dos mil quetzales.

b) Alteración de programas: consiste en alterar, borrar, o de cualquier modo inutilizar m las instrucciones o programas que utiliza el computador y lo relaciona con una pena de prisión de de seis meses a dos años y multa de dos mil quetzales.

c) Reproducción de instrucciones o programas de computación: Copiar o de cualquier modo reproducir las instrucciones o programas de computación sin autorización del autor y lo relaciona con una pena de prisión de seis meses a cuatro años y multa de quinientos a dos mil quetzales.

d) Registros prohibidos: consiste en crear un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas y lo relaciona con una pena de prisión de seis meses a cuatro años y una multa de doscientos a mil quetzales.

e) Manipulación de información: Este delito consiste en usar registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para oculta, falsear o alterar los estados contables o la situación patrimonial de una persona o jurídica. Por lo que se establece como consecuencia la

aplicación de una pena consistente en prisión de uno a cinco años y multa de quinientos a tres mil quetzales.

f) Uso de información: Consiste en utilizar u obtener para sí o para otro, datos contenidos en registros informáticos, banco de datos o archivos electrónicos, sin autorización y lo relaciona con una multa de prisión de seis meses a dos años, y multa de dos mil a diez mil quetzales.

g) Programas destructivos: Consiste en distribuir o poner en circulación programas o instrucciones destructivas, que pueden causar perjuicio a los registros, programas o equipos de computación, lo relaciona con una pena de prisión de seis meses a cuatro años y una multa de doscientos a mil quetzales.

h) Alteración maliciosa de número de origen: Consiste en alterar el número proveniente del extranjero de telefonía utilizando exclusivamente para tráfico internacional, o alterar el número de identificación del usuario que origine una llama telefónica, por cualquier mecanismo, lo relaciona con una pena de prisión de seis a diez años.

2.5. Nuevos tipos penales

Actualmente en el Congreso de la República de Guatemala se encuentra una iniciativa de ley, bajo el Número 4055, en la cual se propone la Ley de delitos informáticos en la que se busca crear nuevos tipos penales para la protección de la integridad, la confidencialidad y la disponibilidad de datos y la tecnología de la información. Esta

iniciativa de ley tiene vinculación con el convenio sobre cibercriminalidad, celebrado en Budapest del Consejo de Europa. Dicho convenio fue creado con el objeto de establecer una política penal en común entre los Estados miembros y otros estados firmantes, para prevenir la criminalidad en el ciberespacio.

Esta nueva iniciativa surge para armonizar la normativa penal entre la comunidad internacional y el ordenamiento interno, ya que la comisión de delitos informáticos no se circunscribe únicamente a un territorio determinado, sino van más allá del territorio.

2.5.1. Acceso ilícito

El delito de acceso ilícito hace referencia al ingreso no autorizado a uno o varios sistemas que utilicen tecnología de la información. El bien jurídico que protege este delito es la confidencialidad, ya que al prohibir el ingreso no autorizado la información de un sistema se encuentra protegida por el Estado. El acceso ilícito puede ser una conducta principal o accesoria. "Es principal si la intención del sujeto activo es simplemente la intromisión al contenido de un sistema informáticos. Es accesoria o preparatoria el acceso ilícito, cuando se acceda a un sistema informático para realizar otro tipo de acciones preparatorias de otro delito."[34]

La iniciativa de Ley número 4055 presentada al Congreso de la República de Guatemala, establece: "Artículo 5: acceso ilícito. Quien acceda a sistema que haga uso de tecnologías de la información, sin autorización o excediéndola, será sancionado con

[34] Alvarado, Rolando. Morales, Ronald. **Op. Cit.** Pág. 20

prisión de dos a cuatro años y multa de cien a quinientas veces el salario mínimo legal vigente". Las circunstancias que agravan la pena son: suplantar identidad del destinatario o remitente para acceder al sistema, utilizar medios electrónicos para ofrecer servicios que estos sistemas proveen a terceros sin pagarlos a los proveedores los servicios, afectar claves de ingreso.

Existe en la ley penal figuras delictivas similares al acceso ilícito, por ejemplo el allanamiento y la violación de correspondencia, ya que en ambos existe un ingreso no autorizado a un bien del sujeto pasivo, en el caso del allanamiento, el bien es la morada y en la violación de correspondencia, el bien es la correspondencia.

2.5.2. Daño informático

Doctrinariamente se indica que el daño informático es "Cualquier deterioro o detrimento doloso de bienes, como la antisocial actitud que se revela con la destrucción total o parcial de las cosas, por el perjuicio patrimonial que para el propietario y poseedor significa y por el atentado colectivo que representa toda disminución de medios de riqueza inmediata o potencial."[35]

En sentido general, daño es todo detrimento, perjuicio o menoscabo que por culpa o dolo de una persona provoque a otro en su patrimonio o en su persona. Este daño trae aparejado una responsabilidad civil en relación a lo que establece el Artículo 1645 del Código Civil, Decreto ley 106, del jefe de gobierno de Guatemala, en el cual establece:

[35] **Ibíd.** Pág. 46.

"Toda persona que cause daño o perjuicio a otra, sea intencionalmente, se por descuido o imprudencia, está obligada a repararlo, salvo que demuestre que el daño o perjuicio se produjo por culpa o negligencia inexcusable de la víctima."

Además de la responsabilidad civil, existe la responsabilidad penal por el daño, ya que en el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, en el Artículo 278 establece como daño "Quien de propósito, destruyere, inutilizare, hiciere desaparecer o de cualquier modo deteriorare, parcial o totalmente, un bien de ajena pertenencia, será sancionado con prisión de seis meses a dos años y multa de doscientos a dos mil quetzales." En este delito se limita a la culpa, puesto que indica el propósito, lo cual hace referencia al dolo.

Dentro del proyecto de Ley 4055, presentado al Congreso de la República de Guatemala, establece "Artículo 6. Daño informático. Comete el delito de daño informático quien, sin estar autorizado, alterare, destruyere, inutilizare, suprimiere, modificare o de cualquier modo o por cualquier medio, dañare un sistema que utilice tecnologías de la información o un componente de éste, será sancionado con prisión de cuatro a ocho años y multa de cien a quinientos veces el salario mínimo legal vigente."

Esta figura delictiva busca la protección de la integridad, la disponibilidad y la confidencialidad de cualquier sistema de computación o tecnología de de la información, tráfico de datos, redes, etc. El también llamado sabotaje informático, es regulado por distintas normativas internacionales, puesto que engloba el terrorismo cibernético, el cual es el acto más paradigmático de un daño informático. El terrorismo

cibernético afecta la infraestructura crítica informática que se define como "Los activos, sistemas, redes, físicas o virtuales, que son vitales para la sobrevivencia del Estado. Que su incapacidad o destrucción podría tener un efecto debilitante en la seguridad de la nación, seguridad económica, salud pública, seguridad financiera, servicios públicos, agua, luz, telefonía, o en una combinación de ellos."[36]

En la actualidad, las conductas de los llamados delincuentes cibernéticos se encuentran dirigidas en la creación de virus, que suprimen o alteran archivos ejecutables por otros infectados con el código de éstos. Los virus pueden inutilizar o destruir de manera intencional los datos almacenados en cualquier soporte informático, lo cual constituye el delito de daño informático.

2.5.3. Reproducción de dispositivos de acceso.

Los dispositivos de entrada o acceso son "aquellos que sirven para introducir datos a la computadora para su proceso, los datos se leen de los dispositivos de entrada y se almacenan en la memoria central o interna. Los dispositivos de entrada convierten la información en señales eléctricas que se almacenan en la memoria central."[37]

En el proyecto de Ley 4055 presentado Al Congreso de la República de Guatemala, regula lo siguiente: "Artículo 7. Reproducción de dispositivos de acceso. Quien de manera deliberada cree, utilice, alterare, capture, grabe, copie o transfiere de un

[36] **Ibíd.** Pág. 49.
[37] http.www.proyectoova.webcindario.com/dispositivo_de_entrada.html (Consultado 30 de septiembre de 2017).

dispositivo de acceso a otra similar, o cualquier instrumento destinado a los mismos fines, los códigos de identificación y/o acceso al servicio o sistema que haga su uso de tecnología de la información, que permita la operación paralela, simultánea o independencia de un servicio legítimamente obtenido, será sancionado con prisión de cuatro a ocho años y multa de cien a quinientos veces el salario mínimo legal vigente."

El bien jurídico tutelado que se protege con este delito es la confidencialidad, puesto que al reproducir dispositivos de acceso se busca ingresar al sistema donde están los datos y la información del sujeto pasivo. Este delito suele aparecer en concurso con otros, cuando los delincuentes realizan réplicas de los dispositivos de captura de información de las tarjetas de crédito o débito de los cajeros automáticos se comete el delito de reproducción de dispositivos de acceso y el de estafa o fraude informático

2.5.4. Dispositivos fraudulentos

En el proyecto de Ley 4055 presentado Al Congreso de la República de Guatemala, regula lo siguiente: "Artículo 8. Dispositivos fraudulentos. Quien produzca, utilice, comercialice u ofrezca sin autorización o causa legítima, uno o varios programas informáticos, equipo, material o dispositivo cuyo uso principal sea el de emplearse como herramienta o medio para cometer los delitos regulados en la presente ley, se sancionará de la manera siguiente: a) Con pena de tres a siete años de prisión para el solicitante; b) Con pena de cuatro a ocho años de prisión para el productor; c) Con pena de cuatro a ocho años de prisión para el que comercializa u ofrece; d) Con pena de tres a siete años de prisión para el que lo utiliza; Cuando no exista concurrencia de las

agravantes específicas mencionadas, se aplicará la de mayor penalidad. Además de la pena de prisión que corresponda, el delito será sancionado con multa de cien a setecientas veces el salario mínimo legal vigente."

La conducta prohibida gira en torno a los verbos rectores de producir, utilizar, comercializar u ofrecer medios electrónicos o de tecnología de la información, para cometer delitos informáticos, es por ello que este delito es accesorio, ya que para su comisión es necesario que el medio que se cree, sea usado principalmente para cometer los siguientes delitos: acceso ilícito, daño informático, reproducción de dispositivos de acceso, espionaje informático, violación a la disponibilidad, fraude informático, interceptación ilícita, falsificación informática, control de acceso de pornografía infantil, difusión y alteración de imágenes personales, uso de identidad ajena, delitos contra la nación y los actos de terrorismo.

2.5.5. Espionaje Informático

El espionaje es la obtención encubierta de datos o información confidencial. Es determinado como delito, puesto que tal conducta representa una violación a los derechos individuales de las personas específicamente a su intimidad. El espionaje se da a través de dos técnicas: la infiltración y la penetración. La infiltración "es la técnica usada para introducir individuos en el bando contrario o enemigo con el fin de conseguir información relativas a planes, actividades y proyectos."[38] Y la penetración que es "la técnica cuyo objetivo es conseguir la colaboración consciente o inconsciente de un

[38] Jarabo Valdivieso, Pablo. **El espionaje pasado y presente.** Pág. 3.

miembro de la organización o grupo contrario para que suministre datos e información secreta del grupo que forma parte."[39]

En el proyecto de Ley 4055 presentado Al Congreso de la República de Guatemala, regula lo siguiente: "Artículo 9. Espionaje informático. Comete el delito de espionaje informático quien, sin estar facultado para ello, se apodere, obtenga, revele, trasmita o difunda el contenido, parcial o total, de sistema que utilice tecnologías de la información o dato informático, de carácter público o privado, será sancionado con prisión de seis a diez años y multa desde doscientas a setecientas veces el salario mínimo legal vigente."

En el delito de espionaje informático, el bien jurídico tutelado es la información, en su atributo de la confidencialidad, ya que previene la divulgación de información a personas o usuarios no autorizados. Las herramientas utilizadas para espionaje informático son diversas, ya que son necesarias para la comisión del delito; El hardware a través de adaptadores, de dispositivos y de teclados especializados. El Software a través de programas que se alojan en el núcleo del sistema.

2.5.6. Violación a la disponibilidad.

La disponibilidad, parte del concepto de disponer, el cual es un término con el cual se da la facultad de usar o utilizar determinado bien o cosa. Esta facultad se origina por un derecho de propiedad o posesión de determinado bien. En el ciberespacio, al igual que

[39] **Ibíd.** Pág. 3.

en el mundo físico, existen bienes de dominio público y de dominio privado. Por lo que el uso de las redes y sistemas informáticos debe estar delimitado dentro del dominio público, y en lo privado de lo que se esté autorizado. La disponibilidad "Constituye una característica de la información para garantizar que ésta se encuentre disponible para quien tiene la autorización de acceder a ella, sean persona, procesos o aplicaciones en cualquier momento."[40]

La disponibilidad en la informática asegura la información y garantiza que esta de encuentre disponible para que las personas autorizadas, la posean en el lugar y tiempo que deseen. Es necesario para que se garantice la disponibilidad, que existan sistemas de control por los cuales se monitorea y revisa los incidentes de seguridad, niveles de servicio y el rendimiento del sistema a tiempo.

En el proyecto de Ley 4055 presentado Al Congreso de la República de Guatemala, regula lo siguiente: "Artículo 10. Violación a la disponibilidad. Quien por cualquier medio provoque la denegación de acceso a redes, información y sistemas que utilicen tecnologías de información, a las personas que están legitimadas para hacerlo, se sancionará con pena de seis a diez años de prisión y multa de cien a quinientas veces el salario mínimo legal vigente."

La protección a la disponibilidad debe partir de la prevención de ataques de denegación de servicio, los cuales buscan dejar indisponible un recurso como una página de

---

[40] Alvarado, Rolando. Morales, Ronald. **Op. Cit.** Pág. 258.

internet, aplicaciones, servidores, etc. Por la naturaleza de los medios electrónicos y/o digitales la disponibilidad de la información es sumamente importante.

2.5.7. Fraude informático

El fraude o estafa está tipificada en el código penal, decreto 17-73 del Congreso de la República de Guatemala, por el delito de estafa propia el cual establece en el Artículo 263: "Comete estafa quien, induciendo a error a otro, mediante ardid o engaño, lo defraudare en su patrimonio en perjuicio propio o ajeno." En la descripción es importante resalta que el bien jurídico que se protege es el patrimonio, puesto que el resultado de inducir a error a un tercero causa una afectación patrimonial.

En el caso del fraude informático se hace referencia al artificio tecnológico o manipulación del sistema de información; estos como medios necesarios para consumar la cualquier transferencia patrimonial en perjuicio de un patrimonio. Es exactamente el objeto del engaño en donde encontramos la diferencia entre el fraude o estafa y el fraude informático, ya que en la estafa se induce a error a la persona, mientras que en el fraude informático es el sistema informático. El cibercrimen actualmente tiene motivos financieros, por el desarrollo de las relaciones comerciales.

En el proyecto de Ley 4055 presentado Al Congreso de la República de Guatemala, regula lo siguiente: "Artículo 11. Fraude informático. Quien, para obtener algún beneficio para sí mismo o para un tercero, mediante cualquier artificio tecnológico o manipulación del sistema que haga uso de tecnologías de la información, o, a sus componentes, procure la transferencia no autorizada de cualquier activo patrimonial en perjuicio de

otro, será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente.

El bien jurídico que protege este delito es la integridad y de forma particular el patrimonio. La integridad en relación a la unidad de los sistemas informáticos, los cuales son afectados por los artificios tecnológicos y la manipulación de los sistemas. El patrimonio en relación al resultado del delito, ya que termina en un perjuicio al patrimonio de otra persona por las trasferencias no autorizadas. En la actualidad, el fraude informático se puede dar a través de subastas en línea, estafas nigerianas y *phishing.*

"Las subastas al publico constituyen un mecanismos de ofertas al público, en la cual las personas presentan sus pujas electrónicas y estas ofrecen mercancías no disponibles para la venta y exigen su pago antes de la entrega o adquieren mercancías y solicitan su envío, sin intención de pagar por ellas."[41]

La estafa nigeriana es un engaño en el cual se realizan operaciones aleatorias y en la que se maneja como un juego de lotería a cambuí de aportar una determinada suma de dinero; en el cual pierde su inversión y al proporcionar los datos de su cuenta bancaria esta puede ser usada para actos delictivos.

"EL *phishing* se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. El *phiisher,* se hace pasar una persona o empresa de confianza, en una aparente comunicación oficial

---

[41] **Ibíd.** Pág. 87.

electrónica; por lo común un correo electrónico, algún sistema de mensajería instantánea o, incluso, utilizando también las llamadas telefónicas." [42] El resultado de esta acción es el robo de identidad y datos confidenciales, pérdida de productividad y consumo de recursos.

2.5.8. Interceptación ilícita.

Interceptar hace referencia a interrumpir, obstruir, detener una vía de comunicación. En el caso de la informática, los sistemas son un conjunto de redes interconectadas por medio de las cuales se administra la información, y es en estas redes en las cuales puede existir una interrupción, a través de programas o sistemas por los cuales se busque obtener información, sea cual sea su contenido y su objeto.

"En términos de informática, el objeto de la interceptación lo constituye la transferencia de datos informáticos, los cuales son definidos como toda representación de hechos, instrucciones, caracteres, información o conceptos expresados de cualquier forma que se presente a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función."[43]

En el proyecto de Ley 4055 presentado Al Congreso de la República de Guatemala, regula lo siguiente: "Artículo 12. Interceptación ilícita. Quien intercepte de forma deliberada e ilegítima por cualquier medio datos informáticos en transmisiones

[42] **Ibíd.** Pag. 88.
[43] **Ibíd**. Pág. 61.

restringidas, dirigidas u originadas en un sistema que utilice tecnologías de la información, incluidas las emisiones electromagnéticas provenientes o efectuadas dentro del mismo, que transporte dichos datos informáticos, será penado con prisión de seis a diez años y multa de cien hasta mil veces el salario mínimo legal vigente."

El bien jurídico que se pretende proteger con este delito es el la información en su atributo de confidencialidad, puesto que con la interceptación de datos informáticos, el contenido es lo que queda expuesto al uso arbitrario y no autorizado que le dé el sujeto activo de la conducta delictiva.

2.5.9. Falsificación informática

La falsedad es todo aquello que no es verdadero, o su contenido no refleja la realidad, es decir que es algo irreal o no autentico. La falsedad significa poner lo falso en lo que debiera ser verdadero. La falsedad tiene dos maneras de manifestarse: la primera es mediante la simulación que es cuando representa algo fingiendo o imitando lo que no es real, en este caso existe una sustitución total de lo verdadero; la otra es mediante a alteración que supone la modificación de la esencia de algo, se altera algún elemento del objeto verdadero por lo que existe una sustitución parcial de lo verdadero.

En el ordenamiento penal, específicamente en el Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, existen dos tipos de falsedad en documentos: la falsedad material y la falsedad ideológica. En el caso de la falsedad material es el delito por el cual se crea en todo o en parte un documento público falso o

alterar uno verdadero, de modo que pueda resultar en perjuicio. La falsedad ideológica es insertar o hacer insertar declaraciones falsas en un documento público.

En el caso de la falsificación informática es "la simulación o alteración de datos contenidos en un sistema informativo donde existen otros factores de fuente de información."[44] El bien jurídico tutelado por este delito es la información, puesto que con una falsificación los datos informáticos, los sistemas informáticos sufren perjuicio, ya que sus usuarios pueden caer en error, colocando su información privada en bases de datos no autorizadas poniendo en riesgo su intimidad o su patrimonio.

En el proyecto de Ley 4055 presentado al Congreso de la República de Guatemala, regula lo siguiente: "Artículo 13. Falsificación informática. Quien, a través de cualquier medio copie, altere o sustituya, deliberada e ilegítimamente, datos informáticos de un sistema que haga uso de tecnologías de la información o uno de sus componentes, generando un resultado no autentico o para inducir a usuarios a la provisión de datos personales y/o financieros, será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente."

Los datos informáticos son aquellos hechos que describen los sucesos los cuales son representados a través de símbolos los cuales pueden ser comunicados por letras, números, gestos, etcétera. Los datos informáticos cuando se encuentran procesados se les determina información. La información en su atributo de la integridad es el bien jurídico que se protege con este delito. En este caso, la información son todos los

---

[44] **Ibíd.** Pág. 93.

archivos, bases de datos, documentos, textos, imágenes, voz y video los cuales están codificados en forma digital y se encuentran en un sistema informático.

Las falsificaciones informáticas se clasifican de la siguiente forma:

Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumento: Las computadoras pueden ser usada para efectuar la falsificación de documentos dentro del comercio. Los dispositivos como las fotocopiadoras computarizadas en color, con rayos laser dieron paso a la falsificación en masa, ya que pueden hacer copias de alta resolución, modificando documentos e incluso pueden crear documentos falsos sin tener que recurrir al original.


SECRETARIA
GUATEMALA, C. A.



CAPÍTULO III

3. Criminalística

La criminalística es una ciencia multidisciplinaria, ya que reúne distintos conocimientos de carácter técnico-científico para determinar el tiempo, modo, lugar del hecho y la identificación de los autores o participes del ilícito o delito. El objetivo de la criminalística es descubrir, estudiar o desvirtuar aquellos elementos materiales recogidos durante la investigación en el lugar del ilícito, para posteriormente someterlo a análisis de las ciencias físicas, químicas o biológicas con el fin de probar una posible conducta punible, con ello coadyuvar a la averiguación de la verdad dentro del proceso penal.

Es necesario diferenciar a la criminalística de otras ramas del saber jurídico-penal como la criminología, la policía científica y medicina forense. La diferencia con la criminología radica en que esta ciencia estudia el comportamiento delictivo y la reacción social que esta provoca, mientras que la criminalística no estudia el comportamiento, sino las circunstancias. En el caso de la policía científica estudia de forma práctica a los criminales y al crimen, mediante métodos científicos de investigación para descubrir los autores de los delitos. La medicina legal se encarga de forma específica al análisis de los aspectos biológicos que auxilian al derecho en la investigación de la verdad.

Al diferenciar a la criminalística de otras ciencias o disciplinas del saber jurídico, podemos partir de definiciones de criminalística para comprender su objeto de estudio.

3.1. Definiciones



Según Juventino Montiel "Etimológicamente la palabra criminalística proviene de raíces latínas como: *crimi* que significa crimen; *ini* que significa grave; *ista* que hace referencia a la actitud, ocupación, oficio o hábito; y *ica* que se refiere a perteneciente a la ciencia o arte." Por lo que se puede definir la criminalística como la ciencia que se ocupa del estudio del crimen grave. En el desarrollo de la criminalística, distintos especialistas la han definido de formas variadas a esta ciencia, extrayendo las siguientes definiciones.

"La criminalística es una ciencia natural y penal, que mediante la aplicación de sus conocimientos, metodología y tecnología en el estudio de indicios o de las evidencias físicas asociativas, descubre y verifica de manera científica un hecho presuntamente delictuoso y a los presuntos autores y sus cómplices; además aporta las pruebas materiales y periciales a los órganos que procuran y administran justicia mediante estudios identificativos y reconstructivos e informes o dictámenes expositivos y demostrativos."[45]

"Disciplina científica que pretende reconocer, identificar, individualizar y evaluar los elementos materiales probatorios (evidencias) mediante la aplicación de las ciencias naturales y sociales a los asuntos de la ley-ciencia, permitiendo descubrir, probar o desvirtuar una presunta conducta punible, es auxiliar del funcionario investigador para definir la condición de víctima o victimario, probar la intervención de uno o varios sujetos y reconstruir el hecho. En este campo confluye el trabajo de muchas y muy

[45] Montiel Sosa, Juventino. **Criminalística 1.** Pág. 31.

variadas ciencias, disciplinas y artes, las cuales admiten un trabajo multidisciplinario y transdisciplinario que permiten observar el fenómeno criminal desde múltiples puntos de vista enriqueciendo la disciplina. "[46]

"Disciplina científica que se dedica al estudio del escenario del delito y las evidencias físicas, mediante su reconocimiento, individualización, identificación y evaluación; se basa en la aplicación de las ciencias en general a la solución de problemas de Ley-ciencia, para descubrir, probar o desvirtuar una presunta conducta punible; facilita al investigador definir la condición de víctima o victimario, demostrar la intervención de uno o varios sujetos y reconstruir los fenómenos ocurridos en el hecho investigado.

Está constituido por las siguientes divisiones: criminalísticas general o teórica; criminalística de campo; criminalística científica o de laboratorio y criminalística estadística. En esta disciplina converge el trabajo de otras muchas y muy variadas ciencias, disciplina y artes, las cuales admiten un trabajo multidisciplinario, interdisciplinario y transdiscursivo, que facilita estudiar el fenómeno criminal de manera multicausal para prevenirlo y combatirlo."[47]

De forma concreta diremos que la criminalística es la ciencia, que a través de conocimientos científicos y empíricos, estudian, analizan y procesan los elementos físicos o materiales dentro de la escena del crimen, para determinar las circunstancias de tiempo, modo, lugar y participación de un hecho considerado como delito; por lo que

[46] Díaz Moncada, José de Jesús. **Lecciones de criminalística.** Pág. 28.
[47] Giraldo Rojas, Juan David. **Criminalística teoría general.** Pág. 101.

auxilia a los operadores de justicia para la averiguación de la verdad, a través del correcto desarrollo de la investigación criminal.

3.2. Origen de la criminalística

El origen de la criminalística se remota a las investigaciones policiacas que fueron el medio para determinar la responsabilidad penal en la comisión de delitos. En un inicio, estas investigaciones carecían del rigor científico como el que se tiene acceso en nuestros días, ya que los investigadores se guiaban por la intuición, el sentido común y la lógica, ya que la investigación giraba en relación a confirmar la culpabilidad de una persona y no a la averiguación de la verdad. "La criminalística tuvo su origen en la obra escrita por el doctor en derecho Hans Gross, titulada *Handbuch für Untersuchungsrichter als System der Kriminalistik,* publicada en Austria en el año de 1892."[48]

La obra que en su traducción al español es: Manual de magistrados para examinar el sistema de la criminalística, fue el producto de la experiencia del autor en relación a los métodos de las investigaciones criminales dentro de lo que llamó criminalística. El interrogatorio, el levantamiento de planos, la utilización de peritos, la interpretación de la escrituras y algunos aspectos sobre las técnicas de engaño y palabras clave utilizadas por los delincuentes contemporáneos fueron los temas fundamentales dentro de su creación, la cual sirvió a los juzgadores para el esclarecimiento de los casos penales ante ellos sometidos.

---

[48] López Abrego, José Antonio. **Criminalística actual ley ciencia y arte.** Pág. 51.

Dentro de la criminalística que desarrolló Hans Gross encontramos las siguientes materias, antropometría, argot criminal, contabilidad, criptografía, dibujo forense, documentoscopia, explosivos, fotografía, grafología, hematología, incendios, medicina legal, química legal y técnicas de interrogatorio.

3.3. Ciencias de la criminalística.

Es necesario hacer hincapié en que la criminalística es el resultado de una evolución dentro de otras ciencias, a las cuales se le conocen como ciencias precursoras. Estas ciencias a través del tiempo han aportado valiosos conocimientos y herramientas para su crecimiento, entre estos sistemas de conocimiento tenemos las ciencias naturales, a las ciencias formales y a las ciencias sociales.

Las ciencias naturales se dividen en ciencias biológicas, ciencias físicas y ciencias químicas. Las ciencias biológicas son aquellas que se dedican a estudiar la vida y sus procesos, desde su origen, evolución y las propiedades de los seres vivos; entre estas podemos mencionar a la medicina, anatomía, psiquiatría, genética etc. Las ciencias físicas son la rama de las ciencias naturales que estudian los sistemas inorgánicos en relación a la energía y la materia, así como al tiempo; en estas ciencias tenemos a la balística, acústica, ingeniería entre otras.

Y por último las ciencias químicas se encargan del estudio, estructura, composición y propiedades de la materia; entre estas ciencias tenemos toxicología, estudio de explosivos y farmacología.

Las ciencias formales son un conjunto sistemático de conocimientos racionales y coherentes, pero cuyos conocimientos pueden ser aplicados a dicha realidad físico-natural; se conforman de de la lógica y de la matemática. Las ciencias sociales como aquellas que estudian al individuo en sus relaciones sociales y las consecuencias que estas relaciones generan; las ciencias sociales precursoras son: el derecho, la psicología, historia, sociología, la política, etc.

"Podemos apreciar que, para la conformación del saber criminalístico, se hace necesario el aporte de todas las ciencias bien sean estas naturales, formales o sociales; esto se debe a que el fenómeno criminal es complejo y mullticausal."[49]

3.4. Objeto de estudio de la criminalística.

Para desarrollar a la criminalística se debe delimitar su objeto de estudio, ya que es de esta manera que identificamos la manera como se investiga y el método de investigación utilizados, los cuales deben ser correspondiente. El objeto de estudio aporta el sistema de problemas a resolver, el método y la metodología deben ser el camino y los pasos más acertados para resolverlos y acercarnos al máximo a la realidad.

"En este objeto de estudio se pueden descubrir datos de gran importancia jurídico-penal situando al investigador en la posición de poder actuar de inmediato. Este objeto de estudio está conformado por dos componentes: Las evidencias físicas también

[49] Giraldo Rojas, Juan David. **Op. Cit** .Pág. 79.

llamadas elementos materiales probatorios y el escenario del delito, también llamado lugar de los hechos."[50] Es necesario hacer análisis de estos dos elementos con el fin de delimitarlos y definirlos, para realizar una correcta aplicación de la criminalística en el proceso de averiguación de la verdad, ya sea como parte juzgadora, acusadora o acusada.

3.4.1. Indicio

Previo a definir la evidencia física y la escena del delito es necesario definir el indicio, ya que este se refiere a la acción o señal que da a conocer algo que es desconocido u oculto. Tiene también un significado de causa y efecto, ya que se le conoce como el antecesor de un acontecimiento. El indicio es entendido como un vestigio, rastro, huella o reliquia

"El indicio es un proceso lógico-racional que permite, a través de un hecho indicador, llegar a una conclusión con mucha aproximación a la realidad. El hecho indicador es imprescindible en el análisis del indicio, y es este el que debe estar respaldado en la evidencia; de tal suerte que lo que resulte cierto es el fáctico, desprovisto inicialmente de cualquier valoración."[51] Por lo que el indicio es un hecho indicador, que no prueba en si mismo nada, pero ayuda de forma eficaz en la investigación para esclarecer los hechos o circunstancias de las que la prueba se pueda obtener.

---

[50] **Ibíd.** Pág. 104.
[51] **Ibíd.** Pág. 104.

Existe una clasificación de los indicios según su grado de certeza, o el tiempo en que fueron producidos ó su relación con el hecho investigado. Por su grado de certeza los indicios pueden ser Indubitados, vehementes, probables y leves. Por el tiempo en que fueron producidos los indicios pueden ser antecedentes, concomitantes y consecuentes. Y según su relación con el hecho investigado los indicios pueden ser determinables, indeterminables, no asociativos y asociativos; y los asociativos pueden subdividirse a su vez en asociativos determinables o indeterminados al momento de someterlos a la cadena de custodia.

3.4.2. Evidencia física, material o probatoria.

"Son elementos físicos que se recaudan por un investigar como consecuencia de un acto delictivo, los cuales pueden servir en la etapa del juicio para demostrar que la teoría del caso que se expone ante el juez es cierta y verificables. Elementos relacionados con una conducta punible que sirven para determinar la verdad en una actuación penal." [52]

La palabra evidencia viene del latín *evidentia* que significa certeza clara y manifiesta de la que no se puede dudar. En relación a lo físico de la evidencia hace referencia a la naturaleza corpórea de los elementos materiales, que sirven para probar la existencia de un hecho o fenómeno. La diferencia entre indicio y la evidencia física es que el indicio debe ser analizado y clasificado según la información que aporta a la

[52] **Ibíd.** Pág. 114.

investigación durante la observación inicial de la escena del delito y luego se someterá a la cadena de custodia.

"En lo general, la evidencia física se obtiene de tres fuentes principales: a) de la escena del crimen, b) de la víctima, y c) del sospechoso y su ambiente."[53] Las evidencias físicas para ser presentadas como pruebas dentro del debate deben tener las características de legalidad, autenticidad, calidad y pertinencia en los cuales sustentará la teoría del caso. Las evidencias físicas permiten probar relaciones entre personas, objetos y lugares, por lo que deben ser estudiados en su naturaleza y composición asegurando su calidad.

3.4.3. El escenario del delito.

El lugar de los hechos o escena del crimen es la fuente principal de indicios para la investigación criminal, el cual puede estar conformado por un espacio abierto, cerrado, mueble o inmueble donde se cometió de forma presunta el delito, al que se debe agregarse los alrededores, áreas adyacentes, lugares relacionados y ruta de escape. La protección de la escena del crimen es vital para que las evidencias físicas que de ella se extraiga tengan validez y puedan ser usadas como pruebas dentro del proceso penal.

En el Artículo 20, del Código Penal, Decreto 17-73 del Congreso de la República de Guatemala indica: "Lugar del delito: el delito se considera realizado en el lugar donde se

[53] **Ibíd.** Pág. 115.

ejecuto la acción, en todo o en parte; en el lugar donde se produjo o debió producirse el resultado y en los delitos de omisión, en el lugar donde debió cumplirse la acción omitida." Encontramos que para el ordenamiento penal, lugar del delito es sinónimo de escena del crimen, puesto que determina el lugar físico en el cual se cometió el hecho ilícito o donde se obtuvo el resultado.

"La escena del delito es cualquier espacio en el cual se halle evidencia física, por medio del cual se facilita la reconstrucción del *itercrimini,* identificar a la víctima, identificar al autor y probar los hechos en juicio, con el objeto de esclarecer un delito"[54]. La escena del crimen es declarada por el ministerio público aplicando procedimientos criminalísticos y la cadena de custodia"

"En el trabajo diario de la criminalística de campo el investigador se ve enfrentado a manejar gran variedad de escenas o lugares donde se ha cometido una conducta punible."[55] La doctrina identifica dos tipos de escena del crimen, como lo son la escena primaria y la escena secundaria. La escena primaria es el espacio donde se encuentra la evidencia fundamental y la escena secundaria es aquella donde se encuentra huellas o rastros dejados por el actor, distantes de la evidencia fundamental o centro de atención pero tienen relación estrecha con la ocurrencia de los hechos investigados.

La finalidad de determinar la escena del crimen "es la búsqueda ordenada y sistematizada de los rastros, vestigios, huellas presentes en el mismo, para que una

[54] **Ibíd.** Pág. 125.
[55] Díaz Moncada, José de Jesús. **Op. Cit.** Pág. 43.

vez que han sido halladas sean señalizadas, fijadas, levantadas, marcadas, embaladas, etiquetadas, aseguradas y remitidas al laboratorio para su debido análisis e interpretación."[56] Esto se resume en la necesidad de de establecer la relación entre los hechos que se investigan y presentarlo dentro del proceso penal como elementos materiales de prueba.

3.5. Principios de la criminalística

La criminalística utiliza para sus procesos de investigación en relación a la escena del crimen y sobre las evidencias físicas, unos principios básicos por los cuales facilitaran al investigador a ver más allá de lo evidente, para someter la hipótesis del caso a verificación a partir de las evidencias físicas encontradas y del resultado de los análisis. Estos principios tienen origen en la lógica y ciencias como la física o las matemáticas por lo que se aplican en las ciencias forenses y la criminalística.

Los principios son los siguientes:

Principio de uso: principio por el cual se establece que en todo hecho, intervienen o se utiliza agentes físicos, químicos y biológicos. En el uso de estos agentes se logra identificar las herramientas utilizadas en la comisión del delito tanto del agresor o de la víctima, es decir se identifican las causas de los fenómenos que se observan en la escena del delito.

---

[56] López Abrego, José Antonio. **Óp. Cit.** Pág. 655.

Principio de producción: Luego de identificar los agentes, en relación a la teoría de causa y efecto, estos producen resultas, huellas o impresiones que deben ser procesados como evidencia física para esclarecer los hechos. Este principio se basa en los efectos que causa el uso de los agentes determinados como causa.

Principio de intercambio: En relación a este principio, en el manejo de agentes y objetos existe un intercambio o transferencia entre el lugar de los hechos, las personas que intervienen en este. Los objetos, personas y lugares tienen vestigios intercambiados siempre que dos objetos entran en contacto material.

Principio de transferencia: Principio por el cual se indica en el cual los las personas o los agentes, transfieren parte material hacia un lugar determinado sin llevarse nada de esta.

Principio de correspondencia: Principio que indica que cuando se utiliza un objeto o agente vulnerarte, siempre se produce marca o huella característica que corresponde con exactitud a la superficie del elemento utilizado.

Principio de identidad: principio por medio del cual se afirma que un objeto, persona o lugar se identifica por sus cualidades cualitativas y cuantitativas, los cuales determinan el ser. Esto quiere decir que no existe un objeto, persona o lugar con las mismas características cualitativas y cuantitativas. Y de existir un objeto, persona o lugar con estas características nos estaríamos refiriendo al mismo objeto que se detalla como indicio o evidencia.

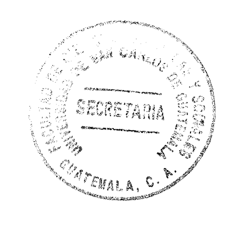
Principio de probabilidad: Principio que indica que en la medida que se conoce los resultados y las causas por las que se produjo este, si se realizan en las mismas condiciones estas tienen que dar el mismo resultado o uno aproximado. Es un principio de carácter predictivo, pero basado en la repetición de las condiciones para provocar un resultado esperado.

Principio de reconstrucción de hechos o fenómenos: Principio que consiste en unir todos los elementos analizados dentro del caso, los fenómenos identificados, las evidencias físicas, todas las circunstancias de tiempo, lugar y modo, para alcanzar un conocimiento completo del delito, para poder reconstruirlo en una línea de tiempo fiel para recrear lo que ya sucedió.

Principio de certeza: Principio de la criminalística por el cual se asegura que la certeza proviene de la hipótesis que mejor se sustente o verifique con las evidencias físicas disponibles y no presenten contradicciones.

3.6. Procesamiento de la escena del crimen

En el manual de normas y procedimiento para el procesamiento de la escena del crimen, del Ministerio Público, se determina una serie de fases por medio de las cuales el equipo multidisciplinario (formado por personal policial, de investigación, técnicos en inspecciones oculares u médicos forenses; todos bajo la dirección funcional del fiscal) realizara la labor de obtener los indicios para realizar la investigación de un hecho delictivo para sustentar un proceso penal.



Las fases en el procesamiento de la escena del crimen son:

Primera fase. Protección y preservación del lugar de los hechos: Tiene por objeto lograr una actuación coordinada y estructurada entre los funcionarios que intervienen en la escena del crimen para asegurar, preservar y proteger el lugar de los hechos hasta la llegada de las unidades especializadas. Procura la protección no solo del lugar de los hechos, sino también de los indicios como personas y objetos que se presuman tenga relación con el hecho ilícito; El propósito de esta diligencia es asegurar la escena del crimen y preservarla con la mínima contaminación y perturbación de la evidencia física.

Segunda fase. Recopilación de la información preliminar: Como su nombre lo indica, en esta fase el personal técnico-científico, previo a iniciar la inspección ocular, en el momento que se tenga conocimiento del hecho delictivo comienza a recolectar todo lo que aporten los testigos, victimas e incluso posibles responsables, policías; El objeto de esta diligencia es la de formar una hipótesis preliminar de los hechos.

Tercera fase: Observación, valoración y planificación: En esta etapa o fase se establece la extensión real de la escena del crimen, con el objeto de efectuar una adecuada planificación de recursos materiales, técnicos y humanos. El objeto de esta fase es asegurar que no exista amenaza en el lugar, desarrollar un correcto abordaje de la escena del crimen para reducir riesgos de daños. La planificación es necesaria para conocer los alcances de la investigación y poder construir de forma previa una hipótesis del caso.

Cuarta fase. Fijación del lugar de los hechos: En esta fase se registran de manera general donde y como se encuentra el lugar de los hechos y se deja constancia formal y oficial de la situación, con vista en los actos procesales y judiciales posteriores. Es en esta etapa en el cual se da la ubicación de personas y objetos dentro de la escena del crimen, el establecimiento de las condiciones del lugar al momento de la llegada, información personal de testigos, víctimas, sospechosos y cualquier declaración y observación.

Quinta fase. Búsqueda y tratamiento de las evidencias: En esta etapa se identifican los métodos de búsqueda de evidencias en el lugar de los hechos que permitan un adecuado manejo de la escena del crimen (método de franjas, cuadricula, zonas o sectores, radial, espiral, punto a punto, técnica libre), buscar técnicamente las evidencias y clasificarlas.

Sexta fase. Liberación del lugar de los hechos: Consiste en verificar la inexistencia de evidencia sin recoger, así como asegura la retirada de restos y el material del equipo técnico; En esta etapa se da la última reunión de los especialistas que han intervenido en la inspección ocular y revisión del trabajo realizado, examen final para determinar elementos de interés, verificación del personal, comprobar que los indicios estén debidamente reseñados, comprobar el levantamiento de residuos materiales y fotografías finales del estado del lugar de los hechos. En esta etapa se quita el acordonamiento de la escena del delito o del crimen. Es necesaria la revisión previa a la liberación para evitar contaminación de la evidencia que este oculta.

Séptima fase. Documentación y remisión de evidencias: en esta etapa se levanta una serie de documentación que tiene por objeto la de garantizar la correcta utilización de la información que sea posible recuperar del lugar de los hechos, las actividades que se realizaron por los especialistas en el estudio de la escena del crimen y la observancia de los requisitos procesales que garantizan la protección y conservación de las evidencias. Estos documentos son: fotografías, imágenes, videos, documento de cadena de custodia, croquis del lugar de los hechos. En relación a las evidencias estas deben ser embaladas, procedimiento por el cual se protegen y conservan los indicios manteniendo su identidad y la integridad de los mismos, e identificadas para luego remitirlas a un lugar adecuado para su correcta conservación hasta el día del debate.

3.7. Cadena de custodia

"Es el procedimiento que garantiza la autenticidad de los elementos materiales probatorios recolectados y examinados, asegurando que pertenecen al caso investigado, sin confusión, adulteración o sustracción. Es desplegado por los funcionarios y personas bajo cuya responsabilidad se encuentran lo elementos probatorios, iniciándose con la autoridad que inicialmente protege la escena del crimen, quien los recauda y finaliza con los diferentes funcionarios judiciales. Implica que estos elementos materiales probatorios se mantendrán en lugar seguro y protegidos, sin que puedan tener acceso a ellos personas no autorizadas."[57]

Los elementos esenciales de la cadena de custodia son:

[57] Díaz Moncada, José de Jesús. **Op. Cit.** Pág. 81.

a) Son una herramienta que asegura y garantiza la seguridad, preservación e integridad de los elementos de prueba recolectados.
b) Debe existir un registro minucioso de la posesión de las evidencias físicas
c) Se deben ubicar las evidencias, en un lugar seguro y autorizado para el efecto, para evitar su contaminación.

La importancia de la conservación de la cadena de custodia es la identificación de evidencias, y que al momento de presentarlo ante el órgano jurisdiccional se compruebe que estos elementos físicos son los mismos que se obtuvieron en el lugar de los hechos. En el Artículo 186 del código procesal penal, decreto 51-92 del Congreso de la República de Guatemala, indica: "Todo elemento de prueba, para ser valorado, debe haber sido obtenido por un procedimiento permitido e incorporado al proceso conforme a las disposiciones de este código." Respecto a la legislación, si el Ministerio Público no comprueba la debida protección a la cadena de custodia en el manejo de evidencias físicas, estas no pueden presentarse en su momento procesal oportuno como medios de prueba.

En el manual del Fiscal del Ministerio Público, de la República de Guatemala, indica que la cadena de custodia es "el mecanismo a través del cual se asegura que la cosa secuestrada, incautada o recogida, no a sido alterada o cambiada por otra al momento de practicar sobre ella un procedimiento. La cadena de custodia suele ser el primer punto de ataque al que recurrirá la defensa para desvirtuar la valoración de evidencia presentada por la acusación." En dicho manual se indica que los eslabones de la cadena de custodia son:



1. Extracción o recolección de la prueba
2. Preservación y embalaje de la prueba
3. Transporte o traslado de la prueba
4. Traspaso de la misma, ya que a los laboratorios para su análisis, o a las diferentes fiscalías para su custodia.
5. Custodia y preservación final hasta que se realice en debate.

La cadena de custodia consta en un documento en el cual se deja constancia que toda la evidencia localizada en el lugar de los hechos, así como el envío y recepción de la misma en cada dependencia o persona que interviene en su manejo y almacenamiento.

Esto consta en una hoja de papel membretado por el Ministerio Público, en el cual se encuentran una serie de firmas de las personas que intervienen en el manejo de evidencias físicas.



CAPÍTULO IV

4. Aplicación de la informática forense en la recolección de evidencia digital en la escena del crimen en los delitos informáticos

En la actualidad, debido a la expansión en el uso de la informática, es común la comisión de delitos informáticos. En estos casos la evidencia es fácilmente alterable, puesto que la información contenida en un soporte informático puede ser manipulada a distancia y en el momento de la recolección de indicios puede modificarle sustancialmente; provocando con ello una obstaculización en la investigación de la verdad que realiza el Ministerio Público.

Por lo que se hace necesario el estudio y aplicación de la informática forense, como una ciencia auxiliar de la criminalística, para la búsqueda de una metodología en la cual se recojan evidencias digitales, sin alterar o dañar los registros para garantizar la identidad y autenticidad de los mismos con ello resguardando la protección a la cadena de custodia.

La búsqueda de una metodología para recolección de evidencia digital, es vital, puesto que de ella depende la admisibilidad, pertinencia y utilidad de la evidencia que se presentará como medio de prueba dentro de un proceso penal. El manejo de la evidencia física y de la escena del crimen, depende totalmente de la naturaleza de los indicios, en el caso de los evidencia digital tienen características muy especificas, por lo que no puede ser tratada de forma genérica o analógica.



4.1. Informática forense

La Real Academia Española define a la informática como "El conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático y racional de la información por medio de computadoras."[58] Por lo que se puede decir que la informática es una ciencia, que tiene por objeto el tratamiento de información, esta información entendida como un conjunto de símbolos que representan hechos, objetos o ideas, utilizando un medio electrónico como lo es la computadora. La informática como ciencia se encarga de las características técnicas de las computadoras y sus componentes asociados (hardware), los tipos de información y datos que se manejarán como lo son archivos y bases de datos, los procesos y métodos aplicados como los programas (software), y los sistemas de comunicación que permitirán tratar la información a distancia y compartida de forma fiable.

La base de la informática son los sistemas informáticos puesto que son un conjunto de elementos que hace posible el tratamiento automático de la información a través de las computadoras. Las partes de un sistema informático son: componente físico el cual está formado por todos los aparatos electrónicos y mecánicos que realizan cálculos y el manejo de la información, componente lógico el cual se compone de las aplicaciones y los datos con los que trabajan los componentes físicos del sistema, y el componente humano el cual está compuesto tanto por los usuarios que trabajan con los equipos como por aquellos que elaboran las aplicaciones.

---

[58] http://dle.rae.es/?id=LY8zQy3 (15 de octubre de 2017).

La informática además, puede ser utilizada en el campo forense, como objeto de estudio y como prueba. Se aplica al campo forense cuando tiene aplicación en la administración de justicia como una ciencia auxiliar de la criminalística o en relación al uso de esta ciencia en la presentación de medios de prueba dentro de un proceso judicial. "Los sistemas informáticos presentes en una escena del crimen son pruebas potenciales, por ser directamente el objeto del ataque (investigación de ataque informáticos, robo de datos), por ser el medio usado en el acto criminal (acoso, engaño, fraudes), o simplemente como testigo"[59]

"La informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. La informática forense hace entonces su aparición una disciplina auxiliar de la justicia moderna para enfrentar los desafíos y técnicas de los intrusos informático, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso."[60]

La informática forense es la ciencia que aplicando procedimientos estrictos y rigurosos puede ayudar a resolver importantes delitos apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales. "La informática forense tiene además entre sus fundamentos la prevención de peligros, la compensación de daños y la persecución de los autores. Por tanto, las tareas son muy variadas y existen especialidades, algunas de ellas compartidas con el campo de la

[59] Verdú Castillo, Fernando. **La informática como prueba forense.** Pág. 2.
[60] Zuccardi, Giovanni y Gutierrez, Juan. **Informática forense.** Pág. 3.

auditoría informática, que también ha tenido un importante auge en los últimos años."[61] Surge la informática forense como una respuesta que las ciencias forenses le dan a la problemática que representa nuevos escenarios para la comisión de hechos delictivos como lo son los medios informáticos.

4.1.1. Clasificación de la informática forense

Dentro de la informática forense, se tienen distintas ramas para el estudio y análisis de esta ciencia auxiliar de la criminalística como lo son:

Computación forense: "Es la disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso."[62]

Forensia en redes (network forensics): Es la disciplina de las ciencias forenses que basa su estudio en el manejo de protocolos, configuraciones e infraestructura de comunicaciones, en el que se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. "Entendiendo las operaciones de las redes de computadoras, es capaz, siguiendo los protocolos y formación criminalísticas, de establecer rastros, los movimientos y acciones que un intruso ha

[61] **Ibíd.** Pág. 4.
[62] **Ibíd.** Pág. 3.

desarrollado para concluir su acción"[63]. El ejemplo más claro de las redes interconectadas esta el internet, escenario de múltiples hechos delictivos.

Forensia digital (digital forensics): Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos y eventos que se catalogan como delitos informáticos.

4.1.2. Importancia de la informática forense

La importancia real de la informática forense proviene del auxilio que esta debe prestarle a la administración de justicia, y la debida protección que se le de a las evidencias digitales dentro de un proceso de carácter judicial. Es en la recolección de evidencias en donde se debe resguardar la integridad de estas, ya que de ella depende su utilidad como medios de prueba.

La importancia radica en sus objetivos, que son:

a) La compensación de los daños causados por los criminales o intrusos.
b) La persecución y procesamiento judicial de los criminales.
c) La creación y aplicación de medidas para prevenir casos similares.

[63] **Ibíd.**



4.2. Medios informáticos

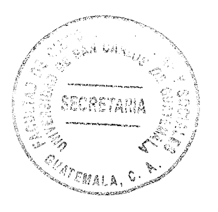
Los medios informáticos "son todos aquellos instrumentos utilizados para almacenar, procesar, transmitir información y datos en formato digital, a través de ordenadores (computadores)." [64] Un medio informático son aquellos objetos que sirven de contendedor de información de carácter general y tiene la función de almacenamiento, procesamiento y transmisión. A diferencia de un medio informático, un medio electrónico son todos aquellos instrumentos creados para obtener un eficiente intercambio de información de forma automatizada.

Tanto los sistemas informáticos, como los medios informáticos son de suma importancia para la informática forense, puesto que estos sirven de medio para la recolección de evidencia digital en el procesamiento de la escena del crimen. En lo que se conoce como la recuperación de datos. En la recuperación de datos, el investigador y los especialistas deben autenticar los datos, asegurarlos, analizarlos y registrarlos. Todo este procedimiento dependerá de la forma en que se encuentren los indicios en la escena del crimen y de la cual se detallará más adelante.

"En materia de delitos informáticos, deben utilizarse herramientas y mecanismos adecuados para poder obtenerla evidencia digital. En esta materia, los ciberdelincuentes son sujetos que tienen un nivel elevado de conocimientos de la materia y por ello tienen, utilizan toda herramienta para evitar dejar rastro."[65]

---

[64] Eyner Isaza, Henry. **Op. Cit.** Pág. 29.
[65] Alvarado, Rolando. Morales, Ronald. **Op. Cit.** Pág. 145.



4.3. Evidencia electrónica y evidencia digital

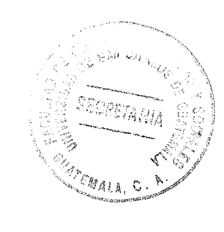
La evidencia electrónica y la evidencia digital no son sinónimos, puesto que se refieren a elementos distintos, pero primero es necesario partir de la definición de cada una de ellas. La evidencia electrónica es "el elemento material de un sistema informático, componente de este o hardware (componente físico)."[66] Y la evidencia digital es "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático"[67]. Por lo que la diferencia es que la evidencia electrónica la constituye el elemento físico como lo son las computadoras, las unidades de almacenamiento interno y externo, etc. Y la evidencia digital por su cuenta es el contenido de la evidencia electrónica, es decir el conjunto de programas, aplicaciones, sistemas operativos, etc.

A diferencia de la evidencia en otro soporte, como lo es el papel, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntica al original, por lo que el principio de identidad de la criminalística se vulnera. Además es potencial el riesgo de realizar copias no autorizadas de archivos, por lo que se crean problemas en la investigación de delitos con relación al robo de secretos comerciales, lista de clientes, material de investigación, archivos de diseño y software en general. La evidencia digital puede encontrarse de las siguientes formas:

a) Contenidas en un archivo (documento, imágenes, e-mails, páginas web, entre

---

[66] **Ibíd.** Pág. 153.
[67] Zuccardi, Giovanni y Gutierrez, Juan. **Op. Cit.** Pág. 8.



otros).

b) En datos logging: registro de actividad de un determinado sistema y son usados para la reconstrucción de eventos.

c) En la metadata: son los datos sobre los datos que no son visibles.

d) Datos de directorio: son informaciones sobre un archivo que conserva en los medios de almacenamiento y contienen datos como nombres, fechas, tamaños, etc.

e) Datos de configuración: son aquellos archivos y datos de directorio que permiten que un computador o una aplicación se comporten de una forma en particular y que puedan proveer evidencia sobre la forma y tiempo en que el computador fue usado.

f) Material forense recuperado: se refiere al material obtenido de medios de almacenamiento que no sería normalmente visto, como los archivos eliminados.

La parte principal del proceso de investigación de la verdad, que desarrolla el Ministerio Público, en materia de delitos informáticos la debe constituir la evidencia digital. Excepcionalmente, cuando el delito tenga relación con los equipos o hardware, debe enfocarse en la evidencia electrónica.

La evidencia digital tiene ciertas características especiales las cuales la diferencian de otro tipo de evidencias, estas características son: la evidencia digital puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original. Esto se hace para no manejar las evidencias originales y evitar el riesgo de dañarlos; y la otra característica es que la evidencia digital es muy difícil de eliminar, ya que existen registros en los cuales el computador almacena los archivos

eliminados, aún cuando estos han sido formateados es posible recuperar la información.

4.3.1. Clasificación de la evidencia digital

Existen tres importantes categorías en las cuales se clasifica la evidencia digital, las cuales son:

Registros generados por computador: Estos las evidencias que son generados como efecto de la programación de un computador. "Estos registros son inalterables por una persona, ya que son generados por programas de seguridad y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema informático que genero el registro."[68]

Registros no generados sino simplemente almacenados por computadoras: Estos registros son generados por una persona y que estos son almacenados en el computador como un documento realizado por un procesador de palabras. En estas evidencias es necesario demostrar la identidad del generador y probar hechos o afirmaciones contenidas en las mismas evidencias.

Registros híbridos que incluyen registros generados por computador así como almacenados por personas en los mismos: En estos registros existe una combinación entre afirmaciones humanas y generadas por computadora.

---

[68] Zuccardi, Giovanni y Gutierrez, Juan. **Óp. Cit.** Pág. 9.



4.3.2. Criterios de admisibilidad de la evidencia digital

Los criterios de admisibilidad de la evidencia dentro de un proceso penal como medio de prueba, tienen relación directa con lo establecido en la legislación guatemalteca, en relación a la legalidad de la obtención de la evidencia, la pertinencia, que no sea abundante y útil y legítima. En el caso de la evidencia digital, para preservar la cadena de custodia y con ello garantizar su validez como medios de prueba, se deben cubrir ciertos criterios avalados por la informática forense para que sean admitidos como medio de prueba las evidencias digitales, tales criterios son: la autenticidad, la confiabilidad, la completitud o suficiencia y el apego y respeto por las leyes de carácter ordinario y reglamentario.

El criterio de autenticidad, tiene vinculación directa con el principio criminalística de la identidad, ya que cada evidencia o indicio tiene una serie de características cualitativas y cuantitativas que la identifican como tal. Una evidencia es autentica en el momento en que se cumplirse con dos elementos esenciales que consisten en demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hechos; y dicha evidencia debe mostrar que los medios originales no han sido modificados, esto en relación a que los registros correspondan efectivamente a la realidad.

Es necesario por ello que se establezcan procedimientos que certifiquen la integridad de los archivos y el control de cambios de los mismos.

El criterio de confiabilidad hace referencia a los registros de eventos de seguridad que adquieren esta característica si provienen de fuentes que son creíbles y verificables. Para comprobar la confiabilidad, es necesaria una arquitectura de comprobación en la cual se demuestre que los registros que genera la computadora puedan ser identificados, recolectados, almacenados y verificados. Una evidencia digital es confiable en el momento en que el sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir almacenar o generar prueba.

El criterio de suficiencia o completitud, la evidencia para ser considerada debe estar completa. Para asegurar esto es necesario contar con mecanismos que proporcionen integridad, sincronización y centralización. Es por ello que el fiscal o el encargado de realizar la investigación tengan una vista completa de la situación, para realizar una correcta correlación de eventos. Y por último el criterio de apogeo y respeto por las leyes y reglas del poder judicial se refiere a que la evidencia digital debe cumplir con el ordenamiento jurídico y legal del país.

4.4 Manejo de evidencia digital en la recolección de evidencia digital.

El correcto manejo de la evidencia digital y su entorno informático es esencial puesto que de este procedimiento depende la validez que el juez le otorgara en el momento procesal oportuno, a las evidencias presentadas como medios de prueba. Es por esto y por la volatilidad de la información contenida en la evidencia digital, que es necesario el desarrollo de una metodología que garantice los medios de investigación de los delitos

informáticos. La metodología que en breve se detallará, puede ser aplicada en el procesamiento de la escena del crimen de los delitos informáticos.

El investigador debe determinar el objeto de la investigación, en este caso desarrollaremos el que hacer con los dispositivos electrónicos que reproducen imagen como lo es un ordenador portátil, un teléfono celular inteligente, una videocámara, un reproductor de video, una tableta electrónica, consolas de videojuegos. Todos estos aparatos electrónicos al contener un sistema informático, pueden constituir evidencia electrónica, y por ende contener evidencia digital.

Cuando se tiene el conocimiento de la comisión de un delito informático, los agentes de la investigación del Ministerio Público, el fiscal encargado de la investigación y los expertos, en el momento de presentarse al procesamiento de la escena del crimen de delitos informáticos deben:

1. Preparar adecuadamente la escena del crimen: en esta fase se debe realizar un plan de operaciones y preparar al equipo a través de herramientas útiles para el procesamiento de escenas del crimen. Se debe contar con herramientas necesarias para lograr el acceso al lugar donde se tienen indicios razonables de la existencia de la evidencia electrónica y digital. Es necesario en este primer paso, que el personal que realice la investigación tenga herramientas forenses y de recolección de evidencias como guantes de látex, bolsas anti-estáticas, etiquetas para prueba y cinta adhesivo, con esto estructurar y documentar la cadena de custodia de los elementos.

2. Asegurar adecuadamente la escena del crimen: en esta etapa es necesario asegurar la seguridad la vida e integridad de las personas que intervengan en el procesamiento de la escena del crimen, como se realiza en cualquier escena.

3. Documentar la escena de registro: para documentar la escena del crimen de delitos informáticos se recomienda fotografiar y registrar todas las acciones que se lleven a cabo y realizar un boceto de la escena que incluya la ubicación de los ordenadores.

4. Registrar e incautar: en el procesamiento de escena del crimen de delitos informáticos esta fase debe ser muy amplia. El registro e incautación debe ser sobre los dispositivos electrónicos y material digital como lo son computadoras, discos duros, dispositivos de almacenamiento portátil, cámaras digitales, reproductores de música y videos, etc.

5. Identificar la evidencia digital: se tiene que realizar una investigación de todos los objetos cercanos a los dispositivos electrónicos, para encontrar evidencia electrónica y digital que se encuentre escondida u ocultada. En esta etapa se pueden realizar entrevista a los usuarios de los ordenadores para descifrar contraseñas de acceso, establecer configuraciones, información a encriptaciones.

6. Fotografía a la evidencia digital: las fotografías en la escena del crimen deben documentar el estado de los dispositivos electrónicos, la configuración y medios periféricos conectados. Todo lo incautado debe etiquetarse. Los cables y cualquier

elemento que se desconecte debe ser identificado para facilitar su posterior conexión.

7. Llevar un adecuado manejo y preservación de la evidencia: la evidencia digital debe estar alejada de transmisiones de radio u otros elementos con interferencia magnética, evitando temperaturas extremas y debe transportarse adecuadamente. El resguardo de la evidencia debe ser desde el momento de su incautación, hasta en su presentación como prueba dentro de un proceso penal.

Para el correcto procesamiento y diligenciamiento de la escena del crimen las personas que intervengan deben de seguir una serie de recomendaciones, que buscan la protección de la evidencia digital. Las recomendaciones son las siguientes:

a) No se debe tomar objetos sin guates de hule para evitar alteración de huellas dactilares existentes en los medios informáticos.

b) Asegurar el lugar.

c) Asegurar los equipos de cualquier tipo de intervención física o electrónica hecha por extraños.

d) Si no está encendido el medio electrónico, no debe encenderse para evitar el inicio de cualquier tipo de programa de autoprotección que provoque daño en la integridad de la información.

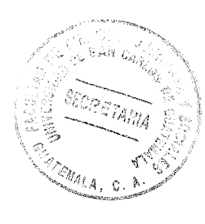
e) Verificar, si es posible, el sistema operativo a fin de iniciar la secuencia de apagado y evitar perdida de información.

f) si se considera razonable, desconectar inmediatamente el equipo informático o electrónico si se considera que está destruyendo la evidencia.

g) Si esta encendido el equipo o medio electrónico, no debe apagarse inmediatamente, para evitar la pérdida de información volátil.

4.5. Propuesta de protocolo de manejo de evidencia digital.

El Ministerio Público, según la investigación realizada en el presente informe, debe de desarrollar un protocolo en el cual se aplique la informática forense de forma técnica para guiar a los investigadores y fiscales en el procesamiento de la escena del crimen, especialmente en el caso de los delitos informáticos. Este protocolo debe desarrollar los medios de investigación, el desarrollo detallado del procesamiento de la escena del crimen de delitos informáticos, las medidas cautelares aplicables dentro del proceso de averiguación de la verdad y la asistencia jurídica mutua en la cual se busque la cooperación internacional en materia de delitos informáticos.





CONCLUSIÓN DISCURSIVA

La recolección de evidencia dentro del procesamiento de la escena del crimen, constituye un procedimiento que el Ministerio Público debe de realizar de forma sistemática y con bases solidas, puesto que de este procedimiento y de la protección de la cadena de custodia, depende directamente la validez de la evidencia que servirá de base para la investigación de un hecho ilícito. En materia informática, por la volatilidad de la evidencia, este procedimiento requiere un protocolo por el cual se establezcan los procedimientos específicos para recolectar evidencia digital de los medios informáticos garantizando con esto, la autenticidad y confiabilidad de estos para que en el momento de presentarlo como medio de prueba, el juez pueda valorarlo en su totalidad.

De la correcta investigación criminal y de la validez de los medios de prueba dentro del desarrollo del proceso penal, depende que el Ministerio Público pueda cumplir con una de sus funciones, el cual es la investigación de los delitos de acción pública y promover la persecución penal ante los tribunales de justicia; esta función se encuentra regulada en la Ley Orgánica del Ministerio Público, Decreto 40-94 del Congreso de la República de Guatemala. Es por ello, que la correcta aplicación de la informática forense en la recolección de evidencia digital, por parte del personal del Ministerio Público en los delitos informáticos es totalmente necesaria.


SECRETARIA
GUATEMALA, C. A.

BIBLIOGRAFÍA

AGUILAR GARCÍA, Ana Dulce. **Presunción de inocencia**. Ciudad de México, México. (s.e.) ed: Colección de textos sobre derechos Humanos, Comisión Nacional de los Derechos Humanos, 2014.

ALVARADO, Rolando; Morales, Ronald. **Cibercrimen.** Ciudad de Guatemala, Guatemala. 1ª ed: Ius-ediciones, 2012.

CRUZ BARNEY, Oscar. **Defensa a la defensa y Abogacía en México.** Ciudad de Guatemala, Guatemala. (s.e.) ed: Instituto de Investigaciónes de la UNAM, 2015.

DÍAZ MONCADA, José de Jesús. **Lecciones de criminalística.** Medellín, Colombia. 1ª ed: Universidad de Medellín, 2009.

EYNER ISAZA, Henry. **Medios electrónicos e informáticos y su implementación al sistema penal acusatorio.** Bogotá, Colombia. 1ª ed: Ediciones Nueva Jurídica, 2016.

GARCIA LAGUARDIA, Jorge Mario. **La defensa de la constitución**. Ciudad de México, México. (s.e.) ed: Instituto de la investigaciones jurídicas, Universidad Nacional Autónoma De México, 1983.

GARCÍA RAMÍREZ, SERGIO. **El debido proceso**. Ciudad de México, México. (s.e.) ed: Editorial Porrúa, 2012.

GIRALDO ROJAS, Juan David. **Criminalística.** Medellín, Colombia. 1ª ed: Universidad de Medellín, 2014.

GONZÁLEZ CAUHAPÉ-CAZAUX, Eduardo. **Apuntes de derecho penal guatemalteco.** Ciudad de Guatemala, Guatemala. 2ª ed: Myrna Mack, 2003.

http://www.dle.rae.es/?id=Y2AFX5s (Consultado 15 de septiembre de 2017).

http.www.proyectoova.webcindario.com/dispositivo_de_entrada.html (Consultado 30 de septiembre de 2017).

http://dle.rae.es/?id=LY8zQy3 (Consultado 15 de octubre de 2017).

JARABO VALDVIESO, Pablo. **El espionaje pasado y presente**. Madrid, España. (s.e.) ed: Ed. Confidential, 2015.

LÓPEZ ÁBREGO, José Antonio. **Criminalística actual.** Ciudad de México, México. (s.e.): ed: Ediciones Euroméxico, S.A. de C.V., 2012.

MONTIEL SOSA, Juventino. **Criminalística 1.** Ciudad de México, México. 3ª ed: LIMUSA, 2010.

RODRIGUEZ BARILLAS, Alejandro. **Manual de derecho procesal penal II.** Ciudad de Guatemala, Guatemala. (s.e.) ed: Instituto de estudios comparados en ciencias penales de Guatemala (ICCPG), 2012.

POROJ SUBUYUJ, Oscar Alfredo. **El proceso penal guatemalteco. t.I.** Ciudad de Guatemala, Guatemala. (s.e.) ed: Magna Terra Editores, 2011.

SANTACRUZ LUMA, Rafael. **El Principio de igualdad entre las partes en el Proceso Penal en México.** Guanajuato, México. (s.e.) ed: Universidad de Guanajuato, 2006.

SOLANO BÁRCENAS, Orlando. **Manual de informática jurídica**. Bogotá, Colombia. (s.e.) ed: Ediciones jurídicas Gustavo Ibáñez, 1997.

VAZQUEZ ROSSI, Jorge Eduardo. **El derecho procesal penal (La realización penal) Tomo I**. Buenos Aires, Argentina. 1ª ed: Rubinzal-Cutzani Editores, 1995.

VAZQUEZ ROSSI, Jorge Eduardo. **El derecho procesal penal (La realización penal) Tomo II**. Buenos Aires, Argentina. 1ª ed: Rubinzal-Cutzani Editores, 1995.

VERDÚ CASTILLO, Fernando. **La informática como prueba forense.** Valencia, España. 2ª ed: Fundación Universitat Empresa. 2015.

ZUCCARDI, Giovanni; Gutierrez Juan. **Informática forense.** Ciudad de México, México. (s.e.) ed: Porrúa, 2012.

Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1986.

Código Procesal Penal. Decreto 51-92 del Congreso de la República de Guatemala, 1994.

Código Penal. Decreto 17-73 del Congreso de la República de Guatemala, 1973.

Ley orgánica del Ministerio Público. Decreto 40-94 del Congreso de la República de Guatemala, 1994.

Ley de delitos informáticos. Iniciativa 4055 del Congreso de la República de Guatemala.

Manual de normas y procedimientos para el procesamiento de la escena del crimen. Ministerio Público, Guatemala. 2013.